Relatório de Políticas de Internet
Brasil 2011

observatório da internet .br
observatório brasileiro de políticas digitais

Centro de Tecnologia e Sociedade
da Escola de Direito do Rio de Janeiro
da Fundação Getúlio Vargas

Comitê Gestor da Internet
no Brasil

Relatório de Políticas de Internet

Brasil 2011

Dados Internacionais de Catalogação na Publicação (CIP)
(Câmara Brasileira do Livro, SP, Brasil)

Fundação Getúlio Vargas. Centro de Tecnologia e Sociedade da Escola de Direito do Rio de Janeiro
Relatório de políticas de Internet : Brasil 2011. -- São Paulo : Comitê Gestor da Internet no Brasil, 2012.

ISBN 978-85-60062-60-7

1. Internet (Rede de computadores) – Leis e legislação – Brasil 2. Observatório Brasileiro de Políticas Digitais 3. Políticas públicas I. Título

12-14693 CDU- 34:004(81)

Índices para catálogo sistemático:

1. Brasil : Internet : Regulação 34:004(81)

Fundação Getúlio Vargas

Relatório de Políticas de Internet
Brasil 2011

observatório da internet .br
observatório brasileiro de políticas digitais

Comitê Gestor da Internet no Brasil

São Paulo
2012

Coordenador editorial
Bruno Magrani

Pesquisadores responsáveis pela pesquisa e redação deste anuário:

CTS-FGV
Bruno Magrani, Carlos Affonso Pereira de Souza, Danilo Doneda, Eduardo Magrani, Giovanna Carloni, Koichi Kameda, Luiz Fernando Marrey Moncau, Marília Maciel, Marília Monteiro, Pedro Augusto Francisco, Ronaldo Lemos e Walter Britto.

CGI.br / NIC.br
Alexandre Barbosa (CETIC.br), Antonio Marcos Moreiras (CEPTRO.br), Caroline Burle dos Santos Guimarães (W3C Brasil), Cristine Hoepers (CERT.br), Klaus Steding-Jessen (CERT.br), Milton Kaoru Kashiwakura (CEPTRO.br), Reinaldo Ferraz (W3C Brasil), Vagner Diniz (W3C Brasil) e Yasodara Maria Damo Córdova (W3C Brasil).

Secretaria Executiva do CGI.br
Hartmut Glaser – Secretário Executivo
Carlinhos Cecconi, Gabriela Villela da Luz, Juliano Cappi e Paula Liebert Cunha

Comunicação NIC.br
Caroline D'Avo, Everton Teles Rodrigues e Fabiana Araujo

Apoio Editorial / DB Comunicação Ltda.
Revisão: Aloisio Milani e Ângela Guanaiss
Projeto Gráfico: Suzana De Bonis
Editoração : Maria Luiza De Bonis

Apresentação

O Comitê Gestor da Internet no Brasil – CGI.br tem sua história construída desde 1995, quando a Internet e a *web* no Brasil ainda eram dimensionadas em não muitos milhares de domínios e o número de conselheiros no comitê contava-se nos dedos da mão. Desde então só temos expandido para além do que se imaginava na ocasião. Não é muito tempo se considerarmos os nem 20 anos da história do comitê. Mas são milhões de domínios depois. Somos também muitos outros conselheiros. Muitos já exerceram seus mandatos em gestões passadas. E muitas são as cadeiras ocupadas pelos atuais 21 conselheiros, representantes de diferentes setores.

Tenho bom orgulho em ser partícipe ativo dessa história, partilhando sonhos e conquistas com tantos outros que desde a origem por aqui já se somaram tecendo uma rede multissetorial, multiparticipativa, multilateral, ou, para usar um vocábulo em inglês, *multistakeholder*, tal como ficou conhecido mundialmente o modelo de governança em organismos plurais e de múltiplos interesses.

Sim, e se há mesmo no múltiplo mundo de hoje algo que se pode identificar como plural, interativo, participativo e colaborativo, se há algo, isso é a Internet e a *web*. Referenciamos vínculos em criativos modos que não podíamos prever antes. Pesquisamos e observamos muitas e várias informações de tanto que sequer sabemos ainda dimensionar o quanto é esse gigantesco tanto de documentos, objetos, aplicações e serviços acessíveis dos nossos dispositivos de navegação.

Pelo tanto que é, e talvez por mais ainda, intensificamos conversas e discussões para o desenvolvimento de políticas e leis voltadas para essa nova dimensão do viver em sociedade: viver em rede na Internet brasileira. Nossas conversas pas-

saram a ser pautadas pela observação dos princípios, direitos e deveres dos usos da Internet brasileira. E foi, portanto, em perfeita hora que nós do CGI.br nos vinculamos em parceria com o Centro de Tecnologia e Sociedade da Escola de Direito da Fundação Getúlio Vargas no Rio de Janeiro (CTS/FGV) para criarmos juntos o Observatório Brasileiro de Políticas Digitais ou, como ficou conhecido, o Observatório da Internet Brasileira.

Não chega a ser uma feliz coincidência, pois somos partícipes e construtores desses novos modos em rede. Mas coincidimos no propósito e reconhecimento da necessária observação. Observação e análise de forma permanente das principais iniciativas de regulamentação da Internet. Observação e identificação das políticas públicas voltadas para a Internet brasileira. Observação e comparação das propostas internacionais, dos modelos de governança da Internet.

E essa publicação que ora entregamos é o resultado de nossas primeiras observações conjuntas do CGI.br e do CTS/FGV. Demos o título de Relatório de Política de Internet – Brasil 2011 e discorremos sobre os projetos de leis e os debates que se sucederam no ano de 2011 sobre as tentativas de dispor sobre crimes na Internet, sobre disciplinar princípios e direitos com o Marco Civil da Internet, sobre neutralidade da rede, sobre banda larga, sobre medição de qualidade, sobre muitos outros temas.

Essa é a primeira publicação sistematizada do Observatório da Internet Brasileira. Não será a única. A própria leitura convidará a novas análises e investigações. Ainda somos muito novos. Nem completamos 20 anos de história do CGI.br e ainda há muito a observar.

Convido você, amigo leitor e internauta, a também fazer as suas observações.

Prof. Hartmut Glaser
Secretário Executivo do CGI.br

A equipe do Centro de Tecnologia e Sociedade da Escola de Direito do Rio de Janeiro da Fundação Getulio Vargas tem o prazer de apresentar o "Relatório de Políticas de Internet – Brasil 2011". Este é o primeiro relatório compreensivo elaborado no Brasil que analisa algumas das mais relevantes propostas legislativas, regulatórias técnicas e de políticas públicas que afetaram a Internet no Brasil durante o ano de 2011. O documento é fruto de uma parceria entre o CTS-FGV e o Comitê Gestor da Internet do Brasil – CGI.br, que criou o Observatório Brasileiro de Políticas Digitais, ou simplesmente Observatório da Internet, como ficou conhecido.

O CTS-FGV foi criado há nove anos com a missão de desenvolver pesquisa interdisciplinar sobre a Internet e a tecnologia digital, produzindo conhecimento para auxiliar no desenvolvimento institucional, econômico, social e cultural da Internet no Brasil. Ao longo destes anos, o CTS-FGV tem colaborado com diversos indivíduos, instituições e governos no processo de discussão da regulação da Internet no Brasil, um papel que posicionou o Centro como um dos principais *think tanks* nesta área. Dessa maneira, o CTS-FGV tem trabalhado em conjunto com o governo brasileiro organizando consultas públicas e elaborando análises sobre leis para regular a Internet, tais como o Marco Civil da Internet a o anteprojeto de lei para proteção da privacidade e dos dados pessoais.

Esse relatório reflete o trabalho de vários pesquisadores que dedicaram incontáveis horas do seu tempo escrevendo sobre um momento único para a política de Internet no Brasil. Mais do que isso, ele mostra um processo altamente democrático de discussão da regulação da Internet no país, que envolveu diversos participantes, sejam eles universidades, empresas, ativistas e indivíduos que realmente se importam com o futuro da sua liberdade na rede. O relatório conta a história da regulação da Internet no Brasil em um dos anos mais ativos. Uma história que temos a alegria de compartilhar com vocês.

Bruno Magrani, Carlos Affonso e Ronaldo Lemos
Centro de Tecnologia e Sociedade da Escola de
Direito do Rio de Janeiro da Fundação Getulio Vargas

1

Crimes na Internet: o Projeto de Lei nº 84/99

Um ponto de partida apropriado à análise da regulação da Internet no Brasil é o Projeto de Lei nº 84 de 1999.[1] Proposto pelo deputado Luiz Piauhylino, para disciplinar crimes cometidos pela Internet, o projeto, que também ficou conhecido como "Lei Azeredo" [2], tornou-se um divisor de águas na regulação da Internet no Brasil, quando gerou uma mobilização social sobre questões de Internet sem precedentes no país.

É interessante notar que esse projeto não foi o primeiro nem o único a prever a tipificação de crimes na Internet. Ao longo das duas últimas décadas, diversos Projetos de Lei foram propostos para regular condutas na Internet, vários prevendo a criação de tipos penais. O próprio PL 84/99 foi resultado, na verdade, do desarquivamento de versão modificada de um projeto de lei anterior proposto em 1996. O que diferenciou esse projeto dos demais – e que causou grande mobilização popular ao seu redor – foi a conjugação da criminalização excessiva de condutas tidas como cotidianas, banais ou indispensáveis à inovação na rede, com a aceleração súbita em seu processo de tramitação, impulsionado especialmente pela bandeira do combate à pedofilia e à pornografia infantil.

Além de criar novos crimes para a Internet, o projeto também criava obrigações de vigilância e ampliava os poderes de investigação da polícia de forma demasia-

---

[1] Disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=15028>. Acesso em 3 de maio de 2012. Ao longo deste capítulo, usaremos os termos "PL 84/99", "PL" e "Lei Azeredo" para fazer referência ao Projeto de Lei nº 84 de 1999.

[2] O nome "Lei Azeredo" deve-se ao seu principal defensor, o deputado federal Eduardo Azeredo do PSDB de Minas Gerais.

da, fato que levou alguns ativistas a denominar o projeto como "AI-5 Digital" [3], em referência ao decreto da época da ditadura militar que suspendeu as garantias constitucionais. O PL 84/99, por exemplo, impunha aos provedores de serviço de Internet e aos provedores de conexão a obrigação de guardar os registros de conexão e de acesso dos usuários pelo prazo de três anos (art. 22, I). Além disso, criava também o dever do provedor informar à autoridade policial de maneira sigilosa sempre que tivesse a suspeita da prática de um crime (art. 22, III). Adicionalmente, redação fruto de má técnica legislativa, criminalizava o acesso não autorizado a um sistema informatizado – tipo que por si inviabilizaria a engenharia reversa, que é fundamental ao processo de aprendizado e de inovação tecnológica (art. 285-A).

De modo geral, ainda que fosse importante coibir a prática de crimes como a pedofilia, disseminação de vírus, dentre outras práticas aviltantes no âmbito da rede mundial de computadores, a redação do PL 84/99 apresentava problemas com relação à sua abrangência e imprecisão, que podiam gerar efeitos colaterais graves.

Estudo do Centro de Tecnologia e Sociedade da Escola de Direito da Fundação Getulio Vargas identificou diversos problemas com relação ao projeto de lei, os quais expomos de forma resumida a seguir.[4] No que tange à abrangência, a intenção do projeto de criminalizar somente condutas graves no âmbito da rede foi extrapolada. Seus dispositivos, mais do que tipificarem condutas criminais, traçavam obrigações de vigilância por parte dos provedores de acesso e de conteúdo e obrigações de disponibilização de dados independentemente de ordem judicial. Essas obrigações representam uma ameaça à garantia de direitos fundamentais dos usuários, como, por exemplo, os direitos à privacidade e ao devido processo legal.

Além disso, a imprecisão da redação dos artigos, por exemplo, ao tratar conceitos relacionados à proteção de dados pessoais com pouco rigor técnico, corrobora para aumentar ainda mais essa ameaça aos direitos fundamentais. Permi-

---

[3] Paulo Rená cita entrevista em que Sergio Amadeu descreve a origem do nome AI-5 Digital: "Dois jovens vieram me entrevistar para o IG e o que estava filmando falou "poxa, mas isso é um AI-5 digital". Era a época do aniversário do AI-5 (o Ato Institucional nº 5 completou 40 anos em 13 de dezembro de 2008) e eu comentava que, quando se transforma exceção em regra e todo mundo passa a ser considerado culpado até que se prove a inocência, tem-se um Estado de exceção. Quando você fala que tem que colher e guardar dados de todo mundo, afirma que todo mundo é suspeito. E serão criadas dificuldades para telecentros, programas de inclusão digital... Você vai em um café, em uma cidade que tem rede aberta, e o gestor da rede vai ser responsabilizado. Ninguém vai querer abrir a rede." SANTARÉM, Paulo Rená. *O Direito Achado na Rede*. p.81. Disponível em: <http://bit.ly/dissertacaoprenass>. Acesso em 18 de julho de 2012.

[4] LEMOS, Ronaldo et al. *Comentários e Sugestões sobre o substitutivo do Projeto de Lei de Crimes Eletrônicos* (PL nº 84/99) apresentado pela Comissão de Constituição e Justiça e de Cidadania. Disponível em: <http://bibliotecadigital.fgv.br/dspace/handle/10438/7719>. Acesso em 16 de julho de 2012.

te ainda que condutas triviais e cotidianas entre usuários da rede mundial de computadores encontrem-se abrangidas pelo tipo penal prescrito pelo projeto, podendo levar à criminalização potencial de condutas de um grande número de usuários, que em sua maioria são consideradas legais no ordenamento ou que são reguladas simplesmente como ilícitos civis em função do seu menor potencial ofensivo.

As críticas feitas ao PL 84/99 apontaram ainda que, considerando o contexto atual da legislação nacional e a redação do projeto, sua aprovação traria riscos consideráveis ao desenvolvimento pleno da Internet no Brasil. Esses riscos se traduzem tanto em um desincentivo à existência de um ambiente propício à inovação, no qual os agentes empreendedores contam com previsibilidade jurídica e lidam com regras civis claras e preestabelecidas, como também por representar uma ameaça à garantia de direitos fundamentais dos usuários.

Para incentivar a inovação, um país precisa contar com regras expressas sobre os limites à responsabilidade dos atores, permitindo segurança e previsibilidade nas iniciativas feitas na rede (tais como investimentos, manutenção de arquivos, bancos de dados, etc.). As regras penais devem ser criadas apenas quando as regras civis se mostrarem insuficientes, sob pena de se elevar o custo de investimento no setor e desestimular a criação de iniciativas privadas, públicas e empresariais na área. É preciso ter especial atenção para que a legislação criminal a ser adotada não seja excessivamente ampla ou vaga, como é o caso do projeto de lei em questão. A excessiva indefinição de termos criminais gera incertezas, especialmente para regular um assunto complexo que demanda definições técnicas prévias, as quais ainda não foram pensadas legislativamente no país. Por esse motivo, o legislador precisa ser cauteloso ao regulamentar a questão, estabelecendo a precisão necessária para garantir os objetivos da lei, mas sem extrapolar limites ou basear-se em conceitos demasiadamente amplos. Além disso, qualquer medida de regulação que autorize o monitoramento de atividades *on-line*, inclusive a guarda de informações dos usuários, deve necessariamente contar com os essenciais freios e contrapesos, que evitam abusos – o que não é visto no projeto em questão.

Essa percepção foi amplamente demonstrada pelos vários agentes envolvidos na discussão da regulação da Internet no país, os quais rechaçaram o PL 84/99, bem como por análises de casos internacionais, deixando claro que o caminho natural de regulamentação da rede, seguido por todos os países desenvolvidos, é, primeiro, o estabelecimento de um marco regulatório civil. Esse deve definir claramente as regras e responsabilidades com relação a usuários, empresas e demais instituições no que diz respeito ao acesso à rede, para que, a partir daí, sejam estabelecidas as regras criminais. O direito criminal deve ser visto como última *ratio*, isto é, o último recurso, adotado quando todas as demais formas de regulação falham.

Uma das principais justificativas utilizadas pelos defensores da aprovação do PL 84/99 foi a suposta necessidade de harmonização da legislação brasileira com a Convenção de Budapeste. Essa convenção, também denominada Convenção do *Cybercrime*, foi criada no âmbito do Conselho Europeu visando estabelecer padrões de combate ao crime *on-line*. Foi aprovada em 23 de novembro de 2001, sem a participação do Brasil, e entrou em vigor apenas em 2004, depois da ratificação de somente cinco países. Ainda que aberta para adesão de qualquer país do mundo, até hoje o texto foi ratificado por apenas mais 25 países, principalmente do Leste Europeu e parte da Europa Central. O texto nunca foi aprovado pelo Brasil, mesmo depois de passar pela análise em diversas casas do governo (dentre elas o Ministério da Justiça, o Gabinete de Segurança Institucional da Presidência da República, o Departamento de Polícia Federal, o Ministério de Ciência e Tecnologia e o Ministério das Relações Exteriores), que consideraram a adequação do texto proposto à luz do ordenamento nacional. Portanto, não se pode tratar o texto da convenção como referência para balizar a legislação pátria. Os países que se comprometeram com essa convenção são, principalmente, países que já cumpriram a tarefa de regulamentar a Internet do ponto de vista civil e, somente depois disso, estabeleceram parâmetros criminais para a rede. Se tentarmos harmonizar nossa legislação com essa convenção que sequer foi aprovada pelo governo brasileiro, corremos o risco de seguir a via inversa: criando primeiro punições criminais, sem antes regulamentar técnica e civilmente a Internet no país.

No que diz respeito ao tema da proteção dos dados pessoais, análise feita por Danilo Doneda demonstrou que a incomunicabilidade entre dados cadastrais e dados sensíveis estabelecida pelo projeto, quando trata da obtenção de dados cadastrais por Autoridade Policial junto aos provedores de acesso e conteúdo, gera dois problemas: [5]

1. "O relator do substitutivo utilizou esta categoria (dados sensíveis), que deve ser preservada e diferenciada para possibilitar uma proteção específica para questões mais delicadas (e, portanto, "sensíveis") de forma excessivamente abrangente, para compreender todo e qualquer dado pessoal que não seja de natureza cadastral. Dessa forma, impossibilita-se a tutela diferenciada para os dados sensíveis, que seriam equiparados aos demais dados pessoais (e, consequentemente, impossibilitando a garantia da pessoa em várias si-

[5] DONEDA, Danilo. *Novo texto do PL sobre crimes cibernéticos embaralha conceitos de proteção de dados*. Disponível em: <http://observatoriodainternet.br/novo-texto-do-pl-sobre-crimes-ciberneticos>. Acesso em 20 de julho de 2012.

tuações de ofensa a seus direitos fundamentais). Rascunha-se, dessa forma, uma normativa impossível de se harmonizar com as tendências internacionais em matéria de proteção de dados pessoais;

2. O segundo é um problema de fundo: a tentativa de associar garantias de proteção a dados pessoais somente aos dados sensíveis é um discurso que, eventualmente, vem à tona nas discussões sobre a matéria no Brasil e que, além de ser impossível de ser conciliado com os direitos fundamentais em questão, como com as normativas internacionais a este respeito, apresenta o grave risco de tornar praticamente inócuas também as demais garantias relacionadas à proteção de dados pessoais."

Esse cenário de ameaças a liberdades básicas dos indivíduos e instauração de um sistema de vigilância na Internet gerou muitas críticas da sociedade ao projeto de lei, resultando em intensa mobilização social.[6] Assim, enquanto a existência do PL 84/99 em si era potencialmente danosa, a reação a ele teve o mérito de reunir em torno de uma causa comum sociedade civil, academia, indústria e outros.

Um dos exemplos mais claros do amplo engajamento social em reação ao PL pode ser visto na petição *on-line* intitulada "Em Defesa da Liberdade e do Progresso do Conhecimento na Internet Brasileira"[7], que reuniu mais de 160 mil assinaturas solicitando a rejeição do projeto pelo Senado Federal. Outro exemplo da participação popular materializou-se no movimento Mega Não![8], que organizou diversas atividades de mobilização na Internet e fora dela contra o PL 84/99.

A reação ao projeto de crimes na Internet, dessa forma, criou uma rede de ativismo digital e participação popular no processo de regulação da Internet brasileira que conseguiu não só reverter o avanço da sua tramitação no Congresso, mas também deu ensejo à criação de importantes iniciativas legislativas para garantir a liberdade na rede e a proteção dos direitos dos usuários. Nos capítulos a seguir, nos dedicaremos a duas das principais propostas legislativas que surgiram a partir desse movimento: O Marco Civil da Internet[9] e a Lei de Proteção aos Dados Pessoais.

---

[6] Um ótimo relato da mobilização social realizado em função do PL 84/99 pode ser encontrado em SANTARÉM, Paulo Renã da Silva. *O Direito Achado na Rede: A Emergência do Acesso à Internet como Direito Fundamental no Brasil*. Disponível em: <http://www.scribd.com/doc/41537075/Dissertacao-O-Direito-Achado-na-Rede>. Acesso em 12 de julho de 2012.

[7] Disponível em: <http://www.petitiononline.com/veto2008/petition.html>. Acesso em 1º de junho de 2012.

[8] Disponível em: <http://meganao.wordpress.com/>. Acesso em 1º de julho de 2012. Pela sua participação no movimento de oposição ao PL 84/99, o movimento Mega Não! recebeu o prêmio Frida, concedido pelo Internet *Governance Forum*. Mais informações em: <http://premiofrida.org/eng/>. Acesso em 12 de julho de 2012.

[9] BRASIL. Projeto de Lei nº 2.126/2011. Disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=517255>. Acesso em 10 de julho de 2012.

Dentre os desenvolvimentos mais recentes do projeto, podemos destacar a realização de duas audiências públicas ocorridas em 2011. A primeira[10], realizada em julho, foi promovida pelas comissões de Ciência e Tecnologia, Comunicação e Informática, de Diretos Humanos e Minorias e de Segurança Pública e Combate ao Crime organizado. Durante essa audiência, representantes do movimento Mega Não! entregaram ao deputado Eduardo Azeredo a petição mencionada. A audiência foi transmitida na *web* e acompanhada através do Twitter sob os *hashtags* #cibercrimes, #AI5Digital e #MegaNão.

A segunda audiência[11], realizada em novembro, contou com convidados de diversos segmentos da sociedade civil e da academia para discutir alternativas à redação do projeto e dos PLs apensados.

Em novembro de 2011, como parte de uma estratégia política para impedir a aprovação do PL 84/99, o deputado Paulo Teixeira, do Partido dos Trabalhadores de São Paulo, em conjunto com outros deputados, propôs o PL 2.793/2011[12], que também dispunha sobre a tipificação criminal de delitos informáticos, mas que o fazia de acordo com sugestões feitas em estudo elaborado pelo Centro de Tecnologia e Sociedade da FGV Direito Rio.[13] A estratégia consistia em aprovar um projeto de lei que contivesse o mínimo necessário para coibir práticas graves cometidas através da Internet e, assim, deixar o restante da regulação da rede para o Marco Civil da Internet. Dessa forma, o novo projeto restringiu substancialmente a criação de novos crimes, bem como delimitou a tipificação desses crimes para abordar as condutas absolutamente indispensáveis – e não condutas cotidianas e banais, como o PL 84/99 fazia. Ele também eliminou a disciplina da guarda de registros de usuários (que foi deixada para o Marco Civil da Internet) e reduziu as penas para cada crime. O deputado Paulo Teixeira, bem como os deputados Luiza Erundina (PSB-SP), Manuela D'Ávila (PCdoB-RS) e João Arruda (PMDB-PR), redatores do PL 2.793/2011, apoiam abertamente o Marco Civil da Internet.

---

[10] Disponível em: <http://www2.camara.gov.br/agencia/noticias/CIENCIA-E-TECNOLOGIA/199848-AUDIENCIA-DISCUTE-PROJETO-SOBRE-CRIMES-NA-INTERNET;-PARTICIPE.html>. Acesso em 3 de março de 2012.

[11] Alguns vídeos da audiência podem ser vistos em: <http://blip.tv/everton137/debate-sobre-crimes-praticados-por-meio-da-internet-no-brasil-incompleto-1472007>. Acesso em 1º de julho de 2012.

[12] Disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=529011>. Acesso em 01 de julho de 2012.

[13] Disponível em: <http://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/7719/coment%C3%A1rios%20ao%20substitutivo%20PL%2088-99.pdf?sequence=1>. Acesso em 01 de julho de 2012.

2

O Marco Civil da Internet

O Marco Civil da Internet[14] é a principal iniciativa de regulação da Internet em tramitação no Congresso Nacional brasileiro. Sua criação está diretamente relacionada à mobilização social que se formou em torno do PL 84/99 e pode ser remontada a um dos principais argumentos utilizados para impedir o avanço desse projeto, o qual tinha como objetivo primordial a instituição de regras criminais para o controle da Internet: a necessidade de realização de uma regulamentação civil prévia que permitisse disciplinar direitos e liberdades dos cidadãos.[15] Com esse propósito, o então presidente Luiz Inácio Lula da Silva, atendendo às demandas da sociedade civil, lançou durante o X Fórum Internacional do *Software* Livre (FISL), em 2009, a iniciativa de propor um "Marco Civil para a Internet brasileira".[16]

Nesse contexto, inspirado nos Princípios para a Governança e Uso da Internet, publicado pelo Comitê Gestor da Internet[17], contando com amplo apoio popular

---

[14] BRASIL. Projeto de Lei 2.126 de 2011. Disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=517255>. Acesso em 12 de julho de 2012.

[15] LEMOS, Ronaldo. *Internet Brasileira Precisa de Marco Regulatório Civil.* Disponível em: <http://tecnologia.uol.com.br/ultnot/2007/05/22/ult4213u98.jhtm>. Acesso em 15 de julho de 2012.

[16] Disponível em: <http://congressoemfoco.uol.com.br/noticia.asp?cod_canal=1&cod_publicacao=30724>. Acesso em 21 de maio de 2012. Neste texto, faremos referência a esta proposta de regulação da Internet no Brasil como Marco Civil da Internet ou simplesmente como Marco Civil. A versão do Projeto de Lei utilizada para a realização das análises presentes neste item é aquela apresentada pelo governo federal ao Congresso Nacional, que está disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=517255>. Acesso em 1º de junho de 2012.

[17] BRASIL. Comitê Gestor da Internet. Resolução 2009-003. Disponível em: <http://www.cgi.br/regulamentacao/resolucao2009-003.htm>. Acesso em 17 de julho de 2012.

e de acordo com orientações do governo, a Secretaria de Assuntos Legislativos do Ministério da Justiça (SAL-MJ), em parceria com o Centro de Tecnologia e Sociedade da Escola de Direito do Rio de Janeiro da Fundação Getulio Vargas (CTS-FGV), deu início a um processo aberto e colaborativo de discussão *on-line* de um anteprojeto de lei para criar uma lei básica para a Internet brasileira. Depois de ampla discussão envolvendo diversos setores da sociedade, o anteprojeto foi finalizado e apresentado ao Congresso Nacional e, até o fim de 2011, tramitava na Câmara dos Deputados sob o número 2.126 de 2011.[18]

Neste item, analisaremos essa proposta de regulação em seus dois principais aspectos: (a) o procedimental, que enfoca a inovação promovida pelo processo de consulta, discussão e participação popular, por meio da rede, na redação do Marco Civil; e (b) o substantivo, que abordará os principais temas tratados no Anteprojeto, tais como responsabilidade de provedores de Internet, guarda de registros de *sites*, dentre outros de relevância para o ambiente digital e seus usuários.

2.1 Uma questão de processo

Uma proposta de anteprojeto de lei para regular a Internet só poderia ser construída na própria rede. Nesse sentido, uma das principais inovações promovidas pelo Marco Civil foi exatamente o seu processo descentralizado e aberto de discussão com a sociedade, utilizando-se de ferramentas disponíveis na própria Internet. Através da adaptação de uma plataforma para criação de *blogs*, conhecida como WordPress[19], foi possível implementar um sistema para receber sugestões e comentários no *site* Cultura Digital.[20]

O processo de consulta pública foi dividido em duas fases. Na primeira, que teve início em outubro de 2009 e durou pouco mais de 45 dias, foi submetido à apreciação da sociedade um texto que continha princípios gerais para a regulação da rede. Estes princípios, por sua vez, foram fortemente inspirados por uma resolução publicada pelo Comitê Gestor da Internet, que elencava "Princípios para

[18] BRASIL. Projeto de Lei 5.403/01. Princípios do uso da Internet — Portal da Câmara dos Deputados. Disponível em: <http://www2.camara.gov.br/atividade-legislativa/comissoes/comissoes-temporarias/especiais/54a-legislatura/pl-2126-11-principios-do-uso-da-Internet>. Acesso em 27 de julho de 2012.

[19] Disponível em: <http://wordpress.com/>. Acesso em 18 de junho de 2012.

[20] Disponível em: <http://culturadigital.br/marcocivil/>. Acesso em 21 de maio de 2012.

a Governança e Uso da Internet no Brasil", também conhecida como o decálogo do CGI.br.[21] Os participantes poderiam detalhar esses princípios e propor novos temas a serem abarcados em uma futura legislação.

Durante essa primeira fase de consulta, foram recebidos mais de 800 comentários, que, sistematizados, traduziram-se no texto do anteprojeto posto em consulta pública na plataforma *on-line* por, inicialmente, mais 45 dias. Atendendo a pedidos diversos, essa segunda etapa foi prorrogada por uma semana e encerrou-se no dia 30 de maio de 2010.

Na última fase, houve aproximadamente 1.200 comentários ao texto. Além de indivíduos e organizações da sociedade civil, participaram também empresas e associações ligadas à indústria cultural e de tecnologia, tanto nacionais como estrangeiras, o que aumentou a diversidade de opiniões e, por consequência, a legitimidade do processo.

Um balanço parcial do debate realizado na metade da segunda fase mostrou que até aquele momento os tópicos mais debatidos diziam respeito à proposta de um mecanismo voluntário que garantisse aos provedores de serviços de Internet a isenção de responsabilidade quanto a conteúdo publicado por terceiros. A referida isenção, porém, teria como condição a adoção voluntária de um mecanismo de resposta a notificações extrajudiciais – tanto daquele que se sentisse prejudicado quanto daquele que desejasse, identificando-se, garantir a permanência de seu conteúdo publicado. No entanto, variadas manifestações apontaram as dificuldades de implementação de um mecanismo dessa natureza, em particular sobre os eventuais riscos a direitos constitucionalmente garantidos, como a liberdade de expressão.

Assim, como evidência de que o debate era de fato aberto e colaborativo, uma nova redação foi elaborada a partir das diversas contribuições recebidas. A responsabilidade dos provedores de serviços de Internet por conteúdos publicados por terceiros ficou condicionada ao recebimento e ao descumprimento de ordem judicial específica, ou seja, somente após a decisão de um juiz os provedores ou equivalentes seriam obrigados a remover conteúdos publicados por terceiros, tais como comentários em *blogs*, *tweets*, fóruns de discussão ou vídeos postados pelos usuários.

---

[21] Disponível em: <http://www.cgi.br/regulamentacao/resolucao2009-003.htm>. Acesso em 13 de junho de 2012.

Além dos comentários na plataforma de discussão *on-line*, o processo de debate público do Marco Civil aproveitou a atividade intensa em outros canais da rede, como as manifestações feitas em *blogs* e no Twitter. Uma busca pela *hashtag* #marcocivil ofereceu, durante o período da consulta, um bom termômetro da intensidade da participação. Muitas entidades, empresas e organizações, bem como alguns indivíduos, enviaram suas contribuições através do *e-mail* de contato do processo. Esses documentos, em sua maioria extensos porque analisavam toda a minuta sob consulta, foram submetidos ao público e abertos também à discussão na plataforma *on-line*. Tal medida reforçou o aspecto transparente e aberto do debate.

Os debates presenciais, organizados pela equipe da SAL-MJ ou de forma independente, bem como as audiências públicas realizadas ao longo das duas fases do processo, em vários pontos do país, tiveram um papel importantíssimo. Tais encontros serviam de fomento ao debate e foram essenciais para a divulgação do Marco Civil.

Com o término do debate público, coube à equipe do Marco Civil, reunindo representantes da SAL-MJ e do CTS/FGV, compilar todos os comentários, identificar as opiniões prevalecentes e fazer as alterações porventura devidas para finalmente apresentar à comunidade o texto que foi encaminhado ao Congresso Nacional.

O Marco Civil radicalizou a natureza democrática do processo legislativo. Ao abrir a possibilidade de qualquer pessoa participar da discussão sobre um futuro anteprojeto de lei, a iniciativa rompeu com o conceito de audiências públicas presenciais como o principal momento em que se dá voz aos interessados no processo legislativo. Em vez de declarar uma suposta obsolescência desses encontros, a plataforma *on-line* terminou por complementar a experiência de debates presenciais oferecida pela audiência pública. Além disso, o processo de audiências públicas e as discussões centralizadas nos corredores e gabinetes dos deputados em Brasília valoriza a atuação de empresas e grupos de interesse que têm os recursos para participar dessas reuniões presenciais. O processo realizado por meio da Internet, por sua vez, ajuda a reequilibrar essa equação, aumentando a participação de setores da sociedade que de outra forma seriam subrepresentados.

Adicionalmente, é importante perceber que alterações fatalmente serão realizadas no texto apresentado ao Congresso Nacional durante a sua tramitação nas casas legislativas. Longe de ser um desvirtuamento da natureza da iniciativa, o fato de se fazer chegar ao Congresso um texto construído durante meses através de comentários realizados na Internet deposita sobre os legisladores a tarefa de

aperfeiçoar algo que não surgiu da inteligência isolada de um gabinete, mas sim de toda uma coletividade.

Dessa forma, ao legislador que for propor alterações no Marco Civil são lançados um desafio e uma revelação: o desafio de melhorar o produto de muitos e a certeza de que suas modificações não passarão despercebidas, pois o texto que resultar do Marco Civil certamente será divulgado amplamente na rede e discutido nos mais diversos fóruns e redes sociais. O amplo grau de transparência nos debates do Marco Civil cria naturalmente marcas de revisão sobre qualquer trabalho legislativo futuro.

Também existe, no processo do Marco Civil, uma questão de princípio. Esse princípio nasce na crença de que a melhor regulação da rede é aquela que se inicia na própria rede e que tem como ponto de partida a afirmação de direitos fundamentais. Por isso, o Marco Civil é eminentemente principiológico. Ele busca traçar as diretrizes, os parâmetros, as pautas que serão detalhadas e desenvolvidas no futuro por legisladores, governantes, magistrados, além de estudantes e pesquisadores de temas ligados ao desenvolvimento da rede.

2.2 Os temas abordados pelo Marco Civil

No que toca à substância, podemos dividir o Marco Civil em seis partes principais: (I) fundamentos, princípios e objetivos; (II) direitos e garantias dos usuários; (III) responsabilidades dos provedores; (IV) guarda de registros por provedores de Internet; (V) neutralidade de rede; (VI) a atuação do Poder Público. Abaixo, analisaremos brevemente cada uma delas.

2.2.1 Fundamentos, princípios e objetivos

O Marco Civil, como lei eminentemente principiológica e seguindo a estrutura da Constituição Federal, estabelece, de início, os fundamentos, princípios e objetivos da disciplina da Internet no Brasil. Essas três camadas constituem os pilares que servirão como base ao processo de interpretação e aplicação tanto do próprio Marco Civil e das futuras legislações para a Internet, como, também – e talvez especialmente –, das futuras situações para as quais não haja previsão legal específica.

O primeiro pilar é constituído pelos fundamentos da disciplina da Internet. São eles: o reconhecimento da escala mundial da rede; os direitos humanos e o exercício da cidadania em meios digitais; a pluralidade e a diversidade; a abertura e a colaboração; a livre iniciativa; e a livre concorrência e a defesa do consumidor.

O segundo pilar é composto por princípios gerais para a Internet, que incluem: a garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição; a proteção da privacidade; a proteção aos dados pessoais; a preservação e garantia da neutralidade da rede; a preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas; a responsabilização dos agentes de acordo com suas atividades nos termos da lei; e, finalmente, a preservação da natureza participativa da rede.

Em seguida, o Marco Civil estabelece os objetivos que devem ser levados em consideração na disciplina da Internet, quais sejam: a promoção do direito de acesso à Internet a todos os cidadãos; a promoção do acesso à informação, ao conhecimento e à participação na vida cultural e na condução dos assuntos públicos; a promoção da inovação e fomento à ampla difusão de novas tecnologias e modelos de uso e acesso; e a promoção da adesão a padrões tecnológicos abertos que permitam a comunicação, a acessibilidade e a interoperabilidade entre aplicações e bases de dados.

2.2.2 Direitos e garantias dos usuários

Além destes princípios gerais que perpassam toda a lógica interpretativa do Marco Civil, o projeto de lei reservou um capítulo específico para dispor sobre os direitos e garantias dos usuários. Enquanto aqueles asseguram a consonância do texto com relação aos valores contidos na Constituição Federal, esse os reforça ao garantir a liberdade de expressão e privacidade nas comunicações.

No art. 7º do PL 2.126/11, o acesso à Internet é tido como essencial para o exercício da cidadania, o que resulta na garantia da inviolabilidade e sigilo das comunicações via Internet, da não suspensão da conexão e da manutenção da qualidade contratada, como visto nos incisos desse artigo.

A garantia da não suspensão do serviço de conexão à Internet, salvo pelo não pagamento do serviço, visa impedir que modelos ultrarrestritivos de combate à violação de direitos autorais, como a lei Hadopi (*Haut Autorité pour La Diffusion des Oeuvres et la Protection des droits sur Internet*) na França, sejam implementados no Brasil. O modelo francês de suspensão da conexão decorrente de violação a direito autoral, conhecido como "resposta gradual" ou "*Three Strikes Law*", consiste em uma proposta de lei para tentar coibir o *download* ilegal de músicas

e vídeos veiculados em redes *peer-to-peer*.[22] A lei prevê que sejam dados três avisos antes de apenar o infrator com a suspensão de seu acesso à Internet.

O primeiro passo, após uma suspeita de violação de direitos autorais comunicada ao órgão administrativo Hadopi, é dar ciência ao usuário de que está potencialmente violando direitos alheios. Caso não remova o conteúdo, o usuário recebe uma notificação formal do órgão e, se persistir, tem sua conexão suspensa enquanto o processo é analisado pelo Ministério Público. Caso a violação seja confirmada, o usuário pode ser punido por meio da proibição de contratar qualquer provedor de acesso pelo prazo de até um ano, além de pena de multa e da possibilidade de ser obrigado a continuar pagando pelo serviço do provedor, ainda que com o acesso cancelado.[23] [24]

O Marco Civil pretende, portanto, evidenciar a importância do acesso à Internet e impedir que procedam a sua suspensão sumária, afastando-se acertadamente da iniciativa francesa, que dispõe de forma contrária. Vale lembrar novamente que o referido dispositivo do Marco Civil faz uma exceção tão somente para casos de suspensão decorrentes do não pagamento do serviço.

2.2.3 A responsabilidade dos provedores de Internet

Um dos pontos centrais do Marco Civil é a regulação da responsabilidade dos provedores. A importância da regulação desse tema está diretamente relacionada aos dois valores que ele visa proteger, quais sejam: a garantia de liberdades na rede e o fomento à inovação. Analisaremos como a responsabilidade de provedores afeta cada um destes dois temas, mas antes é importante entender por que os provedores de Internet são um alvo natural das autoridades governamentais quando se trata do controle de informações e investigações na rede.

Provedores são intermediários no processo de comunicação entre os usuários da Internet e, como tal, gozam de posição privilegiada que lhes dá grande poder

---

[22] Para mais informações sobre a tecnologia *peer-to-peer*, veja: <http://en.wikipedia.org/wiki/Peer-to-peer>. Acesso em 12 de junho de 2012.

[23] Disponível em: <http://legifrance.gouv.fr/affichCodeArticle.do;jsessionid=44FCC56BE74A4FAB1E45C368440683DB.tpdjo16v_3?cidTexte=LEGITEXT000006069414&idArticle=LEGIARTI000021212151&dateTexte=20120518&categorieLien=id#LEGIARTI000021212151>. Acesso em 1º de junho de 2012.

[24] Disponível em: <http://legifrance.gouv.fr/affichCodeArticle.do;jsessionid=44FCC56BE74A4FAB1E45C368440683DB.tpdjo16v_3?cidTexte=LEGITEXT000006069414&idArticle=LEGIARTI000021212156&dateTexte=20120518&categorieLien=id#LEGIARTI000021212156>. Acesso em 1º de junho de 2012.

de fato (ainda que não necessariamente de direito) sobre o que trafega em suas redes. Assim, o emprego de técnicas, como a inspeção de pacotes de dados ou o uso de filtros, possibilita aos provedores restringir, monitorar ou bloquear informações, destinatários e remetentes do processo de comunicação na Internet.

Alguns autores têm denominado esses provedores como *on-line gatekeepers*[25], ou seja, agentes que têm o poder fático de interferir (auxiliando ou prejudicando) no que trafega por suas redes. O Marco Civil adotou uma separação funcional entre os provedores de Internet, categorizando-os em provedores de aplicações (serviços *on-line*) e provedores de conexão (ou acesso) – separação essa que adequa as responsabilidades às funções que cada um desempenha de fato.

Os provedores também são peças-chave para a identificação dos usuários na rede. Tanto provedores de serviço ou aplicações quanto provedores de acesso são necessários para a localização de um usuário na Internet. Assim, por exemplo, ao publicar uma informação em uma rede social – que, segundo o Marco Civil, é um provedor de aplicações – o usuário deixa registrado seu endereço IP. Esse endereço é a primeira parte da informação necessária para se chegar até o usuário final.

A segunda parte consiste em saber qual usuário estava utilizando aquele endereço IP no exato momento em que a informação foi publicada. Isso, por sua vez, só é possível através do provedor de conexão à Internet, que possui os registros de acesso dos seus assinantes. Ainda assim, essas informações permitirão encontrar um dispositivo (computador/cliente) que não necessariamente identificará o indivíduo que efetivamente publicou a informação, o que pode acontecer, por exemplo, se o usuário utilizou um *proxy* ou outra tecnologia de anonimização, se o acesso foi feito a partir do computador de terceiros ou se foi feito a partir de um local de acesso público. Se, por um lado, há diversas dificuldades para a localização de um usuário, por outro os provedores de serviço que hospedam as informações tidas como infringentes são facilmente localizáveis, atraindo para si a atenção das partes que sofreram eventuais danos. É nesse sentido que várias ações no Poder Judiciário brasileiro têm se valido da chamada responsabilização de terceiros.

O instituto da responsabilização de terceiros é utilizado em diversas outras áreas do ordenamento jurídico brasileiro. O Código Civil estabelece, por exemplo,

---

[25] ZITTRAIN, Jonathan. A History of On-line Gatekeeping. *Harvard Journal of Law and Technology*, v. 19, n. 2, p. 253, 2006. Disponível em: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=905862>. Acesso em 12 de junho de 2012.

algumas hipóteses em que terceiros respondem por ações às quais não deram causa[26], tais como: os pais que respondem pelas ações dos filhos menores que se encontram sob sua autoridade ou companhia, o tutor ou curador pelos pupilos ou curatelados, ou ainda o empregador por seus empregados. Nessas hipóteses, a razão para a responsabilização está intimamente ligada a um dever de guarda, vigilância ou custódia entre as partes que, quando não observado, gera a responsabilidade pela imprudência ou negligência daquele dever.

O Código Civil estabelece também uma modalidade de responsabilidade em que o terceiro responde ainda que não haja culpa, desde que "a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem".[27] O Código de Defesa do Consumidor, da mesma forma, determina que fornecedores de serviços ou produtos respondam por eventuais danos causados por seus produtos ou serviços[28], independentemente de culpa (o que é chamado pela doutrina de "responsabilidade objetiva").

Apesar da existência de diversas hipóteses no direito brasileiro em que a responsabilização de terceiros pode incidir, sua aplicação aos provedores de Internet pode ser extremamente prejudicial ao desenvolvimento da rede. A responsabilização excessiva dos provedores de aplicações ou serviço pelos danos causados por seus usuários gera um incentivo para que esses provedores monitorem e censurem quaisquer informações que apresentarem um potencial de gerar riscos de ações judiciais ou sanções governamentais.

---

[26] BRASIL. Código Civil. Lei 10.406/2002: "Art. 932. São também responsáveis pela reparação civil:
I. os pais, pelos filhos menores que estiverem sob sua autoridade e em sua companhia;
II. o tutor e o curador, pelos pupilos e curatelados que se acharem nas mesmas condições;
III. o empregador ou comitente, por seus empregados, serviçais e prepostos, no exercício do trabalho que lhes competir ou em razão dele;
IV. os donos de hotéis, hospedarias, casas ou estabelecimentos onde se albergue por dinheiro, mesmo para fins de educação, pelos seus hóspedes, moradores e educandos;
V. os que gratuitamente houverem participado nos produtos do crime, até a concorrente quantia."

[27] BRASIL. Código Civil. Lei 10.406/2002: "Art. 927. Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo.
Parágrafo único. Haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem."

[28] BRASIL. Código de Defesa do Consumidor. Lei 8.078/1990. "Art. 12. O fabricante, o produtor, o construtor, nacional ou estrangeiro, e o importador respondem, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos decorrentes de projeto, fabricação, construção, montagem, fórmulas, manipulação, apresentação ou acondicionamento de seus produtos, bem como por informações insuficientes ou inadequadas sobre sua utilização e riscos."

Adicionalmente, esse modelo de responsabilidade transformaria uma empresa privada em efetivo agente de censura com poderes para monitorar, julgar e implementar censura prévia sobre os indivíduos sem qualquer instância de recurso ou controle de abusos. Dessa forma, garantir que os provedores de Internet tenham responsabilidade limitada é, na verdade, garantir que o usuário de seus serviços tenha liberdade efetiva para se expressar e se comunicar na rede. Vale notar que isso não implica na não reparação do eventual dano causado, mas tão somente que a responsabilidade recairá sobre o indivíduo que efetivamente causou o dano e não sobre o intermediário do processo.

Um outro valor importante que a limitação da responsabilidade de provedores visa proteger é a inovação na rede. É da própria essência do processo de inovação que as ferramentas e aplicações resultantes gerem consequências inesperadas. Essa afirmação é especialmente verdadeira quando se leva em consideração a natureza participativa e aberta que se quer estimular na Internet, pois, ao oferecer tal tecnologia para o público em geral, os subsequentes usos tornam-se ainda mais imprevisíveis.

Nesse sentido, para estimular que provedores de aplicações criem tecnologias inovadoras, cujos efeitos nem sempre serão previstos, é necessário garantir uma certa limitação à sua responsabilidade, especialmente no que diz respeito aos usos que terceiros fazem da tecnologia. Pamela Samuelson, da Universidade de Berkeley, demonstrou a importância da limitação de responsabilidade dos intermediários desenvolvedores de tecnologia, ao analisar como o caso Sony *v*. Universal[29], que estabeleceu crucial precedente para garantir enorme onda de inovação na área de tecnologia da informação nos EUA a partir da década de 1980.

Nesse importante caso, decidido pela Suprema Corte dos Estados Unidos, a empresa Sony foi considerada inocente pelas gravações de filmes que os usuários de seu videocassete doméstico (o Sony Betamax) possibilitava. A limitação dos riscos do negócio é fator crucial para a inovação. Enquanto empresas bem estabelecidas podem arcar com eventuais custos de processos judiciais, empresas novas de tecnologia (*startups*) não possuem a mesma capacidade financeira e são especialmente suscetíveis a demandas judiciais. Em termos econômicos, a

[29] SAMUELSON, Panela. The Generativity of Sony v. Universal: The Intellectual Property Legacy of Justice Stevens. *Fordham Law Review*, Vol. 74, p. 1831, 2006. Disponível em: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=925127>. Acesso em 30 de junho de 2012.

limitação da responsabilidade dos provedores mantém as barreiras para entrada no mercado baixas e promove a ampla concorrência, valor protegido pela Constituição Federal brasileira.

Talvez os grandes paradigmas internacionais sobre responsabilidade de provedores de Internet sejam o *Digital Millenium Copyright Act* (DMCA)[30] – a seção da lei de direitos autorais dos EUA que lida especificamente com Internet e tecnologia digital – e o *Communications Decency Act* (CDA)[31] – lei norte-americana que regula difamações de materiais indecentes na Internet.

O DMCA criou um sistema amplo para a disciplina de obras intelectuais na tecnologia digital. Essa seção pode ser caracterizada genericamente por estabelecer garantias aos provedores contra a responsabilidade derivada da eventual violação de direitos autorais por terceiros, desde que os provedores respeitem algumas obrigações sobre o tratamento de conteúdo e retirada desse, quando solicitado.

Enquanto provedores de acesso (*Transitory Digital Network Communications*)[32] são geralmente isentos de responsabilidade desde que a comunicação dos dados em sua rede aconteça de forma automatizada, os provedores de serviços *on-line* estão sujeitos à responsabilidade quando não retirarem conteúdo infringente do ar, após a solicitação do detentor dos direitos[33]. Esse modelo é conhecido na doutrina internacional como *notice and take down*, pois estabelece um sistema extrajudicial em que detentores de direitos autorais podem notificar provedores de aplicações ou serviços para que esses retirem de seus *sites* obras protegidas por direitos autorais de titularidade daqueles.[34]

Tal sistema tem sido alvo de diversas críticas pelo efeito inibitório (*chilling effects*) que o abuso do envio das notificações de retirada tem sobre provedores e usuários.[35] Como o gatilho da responsabilidade dos provedores de serviços é o não cumprimento da solicitação de retirada enviada pelo particular, há um incentivo

---

[30] Código Geral dos Estados Unidos, seção 17, parágrafo 512.

[31] Código Geral dos Estados Unidos, seção 47, parágrafo 230.

[32] Código Geral dos Estados Unidos, seção 17, parágrafo 512, item (a).

[33] Código Geral dos Estados Unidos, seção 17, parágrafo 512, item (d).

[34] Para mais informações sobre os sistemas de responsabilidade de provedores presentes no direito norte-americano, veja, por todos, ZITTRAIN, *op. cit.*

[35] Neste sentido, veja o projeto *Chilling Effects Clearinghouse* criado para analisar a procedência de notificações de retirada de conteúdo enviadas por detentores de direitos autorais. Disponível em: <http://www.chillingeffects.org/>. Acesso em 12 de junho de 2012.

claro para que todas as notificações sejam cumpridas, independentemente de qualquer análise sobre sua procedência.

O CDA, por sua vez, difere do DMCA tanto em seu objeto quanto em sua abordagem sobre a responsabilidade e os incentivos dados às partes envolvidas. Em relação ao objeto, enquanto o DMCA aplica-se a obras intelectuais, ou seja, aquelas protegidas por direitos autorais, o CDA tem por objeto informações de caráter difamatório, falso, que envolvam conteúdo explícito para menores e outros. Aqueles de natureza difamatória são os que mais se assemelhariam às hipóteses cobertas pelo Marco Civil. Além disso, o CDA proíbe a equiparação dos provedores de serviços a editores para evitar a aplicação da responsabilidade que geralmente incide sobre estes pelo conteúdo publicado.

O primeiro caso a considerar que provedores de serviço não poderiam ser equiparados a editores e, por isso, não poderiam ser responsabilizados por conteúdos publicados por terceiros foi o *Cubby, Inc. v. CompuServe, Inc.*[36] A corte argumentou que, como o provedor de serviço não realizava controle prévio sobre os materiais postados por terceiros, ele não poderia ser responsabilizado. Esse caso foi futuramente revertido pelo julgamento em *Stratton Oakmont, Inc v. Prodigy Sevices Co.* Porém, o CDA recuperou o entendimento estabelecido em *CompuServe* e deu um passo adiante. Além de garantir a imunidade por conteúdo publicado por terceiro, o CDA estendeu essa imunidade à hipótese em que o provedor tome medidas para, de boa-fé, retirar do ar conteúdo que considere difamatório, danoso, etc.[37] Esse modelo do CDA é chamado de "bom samaritano" (*good samaritan*), pois cria incentivos para que os provedores removam voluntariamente conteúdos tendentes a causar danos sem que, com isso, corram o risco de trazer para si a responsabilidade por aqueles danos.

Levando em conta a experiência internacional e os intensos debates e sugestões feitos durante diversas consultas públicas, o Marco Civil adotou modelo que se

---

[36] Caso 776 F. Supp. 135 da Corte Federal do Distrito do Sul de Nova York (*US District Court for the Southern Distric of New York*), 1991.

[37] As definições do CDA incluem outras hipóteses que constituem variações de condutas obscenas ou indecentes. O texto literal dispõe que:
"47 U.S.C. § 230
(c) (2) *Civil Liability*
No provider or user of an interactive computer servisse shall be held liable on account of –
(A) *any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected*; (...)".

distancia do sistema de *notice and take down* norte-americano, ao garantir imunidade mais robusta aos provedores de aplicações pelos conteúdos gerados por usuários que utilizem seus serviços. Enquanto nos EUA o provedor fica sujeito a eventuais abusos que podem decorrer do uso excessivo de notificações por parte dos detentores de conteúdos *on-line*, o Marco Civil garante que os provedores só serão responsabilizados por conteúdos de terceiros caso descumpram ordem judicial. Assim, a versão original do projeto de lei apresentado ao Congresso Nacional dispunha o seguinte:

> *Art. 14. O provedor de conexão à Internet não será responsabilizado por danos decorrentes de conteúdo gerado por terceiros.*
>
> *Art. 15. Salvo disposição legal em contrário, o provedor de aplicações de Internet somente poderá ser responsabilizado por danos decorrentes de conteúdo gerado por terceiros se após ordem judicial específica não tomar as providências para, no âmbito do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente.*
>
> *Parágrafo único. A ordem judicial de que trata o caput deverá conter, sob pena de nulidade, identificação clara e específica do conteúdo apontado como infringente, que permita a localização inequívoca do material.*
>
> *Art. 16. Sempre que tiver informações de contato do usuário diretamente responsável pelo conteúdo a que se refere o art. 15, caberá ao provedor de aplicações de Internet informar-lhe sobre o cumprimento da ordem judicial.*

É importante notar que o Marco Civil adotou separação funcional entre os provedores de conexão e provedores de aplicações para determinar responsabilidades diferentes para cada um deles. Ambos são imunes, a *priori*, pela responsabilidade dos conteúdos de terceiros, mas se a imunidade dos provedores de conexão é absoluta e não pode ser afastada, a imunidade dos provedores de aplicações, por sua vez, é válida enquanto o provedor cumprir com eventuais ordens judiciais para a retirada de conteúdos.

Algumas das críticas que o projeto recebeu dizia respeito ao fato de que, enquanto os provedores encontravam-se protegidos, não havia garantia ao cidadão contra práticas de censura privada realizadas pelos próprios provedores em função de eventuais acordos celebrados. Não parece ser este o caso, por duas razões: uma de mercado e outra de direito.

Primeiro, quando a aplicação oferecida pelo provedor possibilita a publicação de conteúdos por terceiros, a própria natureza da atividade nos faz crer que é benéfico ao provedor estimular essa publicação e que, por isso, ele terá incen-

tivos para não censurá-los. Se os usuários percebem a publicação ampla e sem censura agregando valor ao serviço, mais usuários migrarão para um dado serviço e a concorrência de mercado auxiliará na promoção da liberdade.

Segundo, para os casos em que a dinâmica do mercado não for suficiente (como, por exemplo, nos casos em que os efeitos de rede forem preponderantes, ou que o incentivo para censurar for maior do que o incentivo para não censurar), existem institutos no próprio ordenamento jurídico brasileiro que impõem limites para resguardar os usuários da censura dos provedores.

Assim, medidas de censura, de restrição injustificada de acesso ou abusivas em geral que decorram de eventuais acordos podem ser consideradas como abuso de direito, o que é coibido pelo Artigo 187 do Código Civil.[38] A natureza da atividade, conjugada com a responsabilidade limitada, coloca os provedores em condições de negociação que fazem crer que eventuais acordos não ocorrerão. Se ocorrerem, os incentivos de mercado, conjugados com os limites de direito, farão com que esses acordos respeitem os direitos dos usuários, sob pena das sanções já previstas no direito civil.

Uma crítica derivada da anterior diz que, na prática, o usuário teria a sua liberdade de expressão reduzida porque somente um número muito baixo de usuários recorreria ao judiciário contra eventuais abusos dos provedores, em função da dificuldade de acesso à justiça. Em resposta a essa crítica, além dos incentivos dos provedores para não censurar, demonstrados acima, a parte final do Marco Civil legitima que a defesa dos direitos seja feita coletivamente. Em outros termos: associações, entidades de representação de classe, o Ministério Público e outras instituições poderão acionar judicialmente provedores que pratiquem condutas abusivas de remoção de conteúdo. Com isso, espera-se criar uma fiscalização difusa dos atos de provedores, ao mesmo tempo em que corrige-se eventuais assimetrias de acesso ao Poder Judiciário.

Adicionalmente, vale notar que, ainda que a proposta acima não seja considerada a ideal do ponto de vista da ampla promoção da liberdade de expressão, não parece que a hipótese oposta seja viável. Por hipótese oposta, entende-se um sistema em que o provedor de aplicações que receba conteúdos de terceiros seja obrigado a permitir a publicação de toda e qualquer informação, a menos que receba

[38] Lei 10.406/2002. (Código Civil).
Art. 187. "Também comete ato ilícito o titular de um direito que, ao exercê-lo, excede manifestamente os limites impostos pelo seu fim econômico ou social, pela boa-fé ou pelos bons costumes".

ordem judicial específica ordenando a sua retirada. Essa restrição provavelmente será considerada inconstitucional, por encontrar forte oposição no princípio da livre iniciativa previsto nos artigos 1º, inciso IV, e 170, da Constituição Federal.

Imaginemos o caso em que um empreendedor resolva criar um fórum fechado para discussão dos episódios da conhecida série de televisão *Game of Thrones*. Como já existem vários fóruns semelhantes na Internet, apontamos que, por hipótese, este teria como diferencial o fato de permitir aos usuários discutir cada episódio em tópicos separados sem a preocupação de encontrar informações de episódios futuros que poderiam desvendar as surpresas que a saga guarda. Para tal, o fórum contaria com a atuação de moderadores que excluiriam todos os comentários inadequados que pudessem desvirtuar o propósito do *site*. Um sistema que obrigasse a publicação irrestrita de conteúdos inviabilizaria não só esse, como diversos outros modelos de negócios que envolvessem a moderação por parte de provedores. Tal sistema constituiria invasão excessiva no âmbito de atuação privada e deveria ser evitado.

Por fim, vale lembrar que a proposta de redação do Marco Civil enviada ao Congresso o coloca como norma geral que se aplica a todos os conteúdos na Internet, sem fazer diferença entre conteúdos protegidos ou não por direitos autorais. Se lei futura disciplinar especificamente questões relacionadas a direitos autorais, ela afastará a incidência do Marco Civil, mas, até lá, agirá como regra geral. Como se percebe, a proposta de disciplina da responsabilidade de provedores da Internet que está sendo discutida no âmbito da reforma da lei de direitos autorais prevê um modelo muito semelhante ao do DMCA norte-americano.

2.2.4 A guarda de registros por provedores de Internet

A guarda de registros de usuários por provedores de Internet é certamente um dos temas mais controversos do Marco Civil. A existência desse assunto no projeto de lei só pode ser entendida quando levamos em consideração o contexto do seu surgimento.

O Marco Civil foi criado, como visto no início deste capítulo, em resposta ao PL 84/99, que propunha estabelecer uma gama de crimes na Internet. Dentre as disposições desse projeto, encontrava-se a obrigação de guardar os registros de conexão e de acesso a aplicações de Internet por até três anos, o que ocasionou a incorporação dessa disciplina no Marco Civil como forma de evitar o avanço da discussão no âmbito penal. Ao incorporar a disciplina da guarda de registros, tomou-se o cuidado de restringir as hipóteses em que o acesso seria possível, bem como limitar o prazo de guarda dos registros.

Em seu art. 5º, VI, o Marco Civil define *registro de conexão* como sendo o conjunto de informações referentes à data e hora de início e término de uma determinada conexão à Internet, além de sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados. O *registro de acesso a aplicações*, por sua vez, é definido no texto como o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de Internet a partir de um determinado endereço IP. O texto do Marco Civil prevê que os registros de conexão e os registros de acesso só podem ser entregues à polícia mediante ordem judicial específica e com fins bem delimitados, deixando claro que tais registros são elementos relevantes para a proteção da privacidade, honra e imagem das pessoas.

Ainda, na provisão de *conexão*, onerosa ou gratuita, é vedado guardar os registros de acesso a aplicações de Internet. Já com relação à provisão de *aplicações* de Internet, é facultada a guarda dos registros de acesso dos usuários. O texto prevê, contudo, a possibilidade de se demandar a guarda de registros de acesso a aplicações de Internet, desde que mediante ordem judicial e desde que se trate de registros relativos a fatos específicos em período determinado, respeitados os direitos dos usuários dispostos na lei.

A necessidade de ordem judicial para obtenção de informações que permitam a identificação do usuário ou para demandar a guarda dos registros de acesso pelos provedores de aplicação anula a possibilidade de que tais dados sejam solicitados tanto pela polícia, quanto pelo Ministério Público, independentemente de ordem judicial. O projeto, contudo, prevê a hipótese de que as autoridades solicitem aos provedores a guarda de determinadas informações, mas condiciona a entrega dos dados a ordem judicial específica.

Com relação ao tempo de guarda dos registros de conexão, o Marco Civil estabelece o prazo de um ano. O objetivo foi encontrar um equilíbrio entre, por um lado, a importância de se guardar registros para viabilizar as investigações policiais e, por outro, a necessária garantia de privacidade do cidadão. O prazo de guarda por um ano encontra-se em consonância com estatísticas recentes de uso de dados de registro de usuários solicitados por autoridades de investigação de países europeus.[39]

---

[39] *Report From The Commission To The Council And The European Parliament Evaluation report on the Data Retention Directive (Directive* 2006/24/EC). Disponível em: <http://ec.europa.eu/commission_2010-2014/malmstrom/archive/20110418_data_retention_evaluation_en.pdf>. Acessado em 3 de março de 2012.

Segundo recente relatório[40], de todos os dados de registro de usuários na Internet utilizados em investigações policiais, cerca de 56% estavam armazenados há cerca de três meses ou menos, 19% tinham até seis meses de existência e 18% encontravam-se guardados há até 12 meses. Em outros termos, 93% de todos os dados requisitados para a investigação policial que estavam guardados encontravam-se armazenados por até um ano, o que indica que o prazo do Marco Civil parece ser suficiente para as demandas da polícia. Limitar a guarda desses dados pelo menor prazo possível é fundamental para garantir a privacidade dos indivíduos.

2.2.5 A neutralidade de rede

Para um debate pormenorizado sobre a regulação da neutralidade rede, remetemos ao item 3 deste relatório.

2.2.6 A atuação do poder público

O texto do Marco Civil dispõe em seu capítulo final sobre a atuação que se espera do poder público, com o objetivo de nortear a atuação de todos os entes federativos no desenvolvimento da Internet no Brasil.

Com vistas a alcançar esse fim, ressalta-se a necessidade de se estabelecer mecanismos transparentes, democráticos e colaborativos de governança, bem como de promover a interoperabilidade tecnológica entre os entes federativos dos serviços de governo eletrônico. O texto orienta os entes, ainda, a darem preferência a tecnologias, padrões e formatos abertos e livres. Nesse trecho, contudo, é possível que o Marco Civil encontre resistência judicial futura, face a decisão liminar de 2004 do Supremo Tribunal Federal, que suspendeu os efeitos da lei do Estado do Rio Grande do Sul que previa tratamento preferencial para a compra de *software* livre.[41]

Além disso, destaca-se o fomento às iniciativas públicas voltadas para a cultura digital e promoção da Internet como ferramenta social. A finalidade dessa previsão é a de buscar incentivar a inclusão digital, reduzir as desigualdades entre as diferentes regiões do país relacionadas ao acesso e ao uso de tecnologias da informação e comunicação, além de fomentar a produção e a circulação de conteúdo nacional.

---

[40] Idem.

[41] Liminar condedida na ADI no 3059, em julgamento pelo Supremo Tribunal Federal.

3

A regulação da neutralidade de rede

O conceito da neutralidade de rede pode ser entendido como um princípio de arquitetura de rede, segundo o qual toda a informação que trafega pela rede deve ser tratada de maneira equânime. Tim Wu explica que "a ideia é que uma rede pública de informações que se pretende o mais útil possível aspire a tratar igualmente todos os conteúdos, *sites* e plataformas. Isto permite que a rede transporte todo tipo de informação e suporte todo tipo de aplicativo. O princípio sugere que as redes de informação são mais valiosas quando elas são menos especializadas – quando elas são uma plataforma para múltiplos usos, presentes ou futuros (para aqueles que sabem mais sobre arquitetura de rede, esta descrição é similar ao princípio de arquitetura de rede conhecido como *end-to-end*)".[42]

Em outros termos, o princípio estabelece que provedores de acesso à Internet[43] não devem bloquear o uso ou limitar a velocidade de tráfego de determinados aplicativos ou conteúdos em sua rede. Da mesma forma, a ideia de que provedores de acesso (as operadoras que oferecem o serviço de acesso à Internet ao

[42] Definição de Tim Wu para neutralidade de rede conforme apurada em: <http://timwu.org/network_neutrality.html>. Acesso em 6 de março de 2012.

[43] Utilizaremos a denominação "provedores de acesso à Internet", "provedor de Internet" ou ainda "provedor de acesso" para denominar as empresas de telecomunicações que oferecem o serviço de acesso à Internet. Apesar da natureza distribuída da Internet em princípio significar que todos que se localizam nas pontas da rede são usuários dela, utilizaremos o termo "usuários" em referência aos consumidores, pessoa física ou jurídica, dos serviços de Internet que não têm o fornecimento de conteúdo ou serviço na rede como sua atividade principal. Do outro lado – e tomando-se em consideração as devidas ressalvas –, chamamos provedores de conteúdo as empresas ou indivíduos que forneçam conteúdos ou serviços para o público através da Internet como sua atividade principal. Mais uma vez, esta diferenciação está longe de pretender ser precisa ou imune a falhas, mas, ao contrário, pretende dar uma ideia geral ao leitor.

usuário final, como NET Virtua, Oi, Telefonica, GVT, etc.) poderiam cobrar valores diferenciados de provedores de serviços ou de conteúdos (as plataformas que oferecem serviços *on-line* como busca, rede social, publicação de *blogs*, vídeo, etc.) para que seus usuários tenham acesso mais rápido ou preferencial a determinado conteúdo ou aplicativo poderia também ser considerada contrária ao princípio da neutralidade de rede. Os defensores do princípio alegam que ele é a principal garantia de que a Internet continuará sendo uma plataforma livre e sem restrições para a inovação.[44] Ele assegura também que as barreiras para a entrada no mercado continuarão baixas, possibilitando que indivíduos e pequenas empresas continuem podendo inovar e competir com empresas estabelecidas.

O debate em torno da neutralidade de rede não é novo. Desde o início dos anos 2000, acadêmicos têm se preocupado com o tema no contexto do princípio mais geral da arquitetura *end to end*.[45] No Brasil, ao menos desde o ano de 2004, há notícias de violações à neutralidade da rede. Um dos primeiros exemplos reportados foi protagonizado pela operadora Brasil Telecom, que bloqueou chamadas telefônicas realizadas a partir de serviços de voz sobre IP (VoIP).[46] Em 2006, o serviço de Internet da operadora Oi, o Velox, começou a censurar determinados conteúdos sob o pretexto de garantir a segurança de seus usuários.[47]

Em uma primeira análise, pode parecer que os provedores de acesso à Internet não teriam incentivos para discriminar pacotes de dados em sua rede. A lógica é simples: a disponibilidade de mais aplicativos e conteúdos torna a rede mais atrativa aos usuários, o que por sua vez gera uma vantagem competitiva sobre provedores que eventualmente os restringem. Apesar disso, ao longo dos últimos anos, os provedores têm mostrado que existem incentivos para promover a discriminação ou o bloqueio de aplicativos ou conteúdos e que eles são suficientes para que tais práticas aconteçam.[48]

Baseando-se em casos concretos ocorridos nos EUA, a prof. Barbara Van Schewick, da Universidade de Stanford, aponta três grupos de situações em que provedores de Internet têm incentivos para discriminar pacotes de dados na rede. Primeiro, provedores podem discriminar pacotes para aumentar o próprio lucro em detri-

---

[44] VAN SCHEWICK, Barbara. *Internet Architecture and Innovation*. Cambridge: MIT Press, 2010.

[45] Neste sentido, ver LESSIG, Lawrence e LEMLEY, Mark A.. *The End of End-to-End: Preserving the Architecture of the Internet in the Broadband Era*. Disponível em: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=247737>. Acesso em 3 de janeiro de 2012.

[46] Vide AFFONSO, Carlos A. Todos os datagramas são iguais perante a Rede! *Revista PoliTICs*.

[47] Vale lembrar que a fusão das empresas Oi e Brasil Telecom ainda não havia acontecido na época desses incidentes.

[48] VAN SCHEWICK, Barbara e FABER, D. Point/*Counterpoint: Network Neutrality Nuances*. *Communications of the ACM*. Nova York, v. 52, n. 2, p. 32, 2009.

mento do serviço do usuário. Assim, há um incentivo claro, por exemplo, para prejudicar aplicativos que compitam com outros serviços prestados pelo provedor, como é o caso das restrições a serviços de voz sobre IP (no caso do provedor também oferecer serviço de telefonia), ou mesmo a limitação ao uso de programas baseados no protocolo *bittorrent* (para o caso de provedores que tenham serviço de *video on demand*). Também pode ser classificada neste grupo a proposta de mudança no modelo de negócios dos provedores de conteúdos de Internet para cobrar desses que seus dados sejam transmitidos de maneira mais rápida aos usuários. Essa cobrança não substituiria o valor já pago por usuários para obter acesso à rede, mas tão somente criaria uma fonte adicional de receita para os provedores. Há muita controvérsia sobre se os provedores deveriam ser livres para implementar tal prática ou se essa deveria ser proibida. Em linhas gerais, de um lado argumenta-se que a receita adicional seria utilizada para aumentar os investimentos em infraestrutura, ampliando a capacidade e a velocidade da rede ou diminuindo os custos de acesso para o usuário.[49] No lado oposto, críticos desta prática argumentam que: a) não há garantias de que os lucros adicionais serão reinvestidos na infraestrutura ou mesmo na redução dos preços; b) ela não maximiza o bem-estar social, pois limita a escolha do usuário; c) essa prática aumenta as barreiras à entrada de novos competidores no mercado e, consequentemente, restringe a inovação.

Provedores também têm incentivos para discriminar pacotes para gerenciar o tráfego na sua rede. Como a maioria dos provedores de acesso oferece o serviço ao usuário final cobrando uma taxa fixa mensal enquanto compra acesso à Internet de outros provedores de acordo com a quantidade de dados trafegados, um aumento no tráfego eleva as despesas daqueles provedores sem aumentar sua receita. Dessa maneira, cria-se um incentivo para degradação no tráfego de aplicativos ou conteúdos que consumam muita banda, como clientes que utilizam *bittorrent* ou *websites* que realizam *streaming* de vídeo. O gerenciamento assim pode funcionar como um analgésico que tem efeito imediato, mas não resolve o problema maior do congestionamento da rede. Que fique claro que a capacidade de gerenciamento de tráfego é fundamental para o funcionamento de qualquer rede. Nos momentos de pico de uso da rede, a falta de gerenciamento pode significar a inutilização de determinados aplicativos. Assim, por exemplo, se um *e-mail* demora dois minutos para ser entregue, em vez de demorar poucos segundos, isso não causará grandes prejuízos nem inutilizará a ferramenta, mas, se ao utilizar um serviço de voz sobre IP o atraso de resposta for superior a um ou dois segundos,

[49] Veja por todos YOO, *C. S. Innovations in the Internet's Architecture that Challenge the Status Quo. Journal on Telecommunications and High Technology Law.* Disponível em <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1472074>. Acesso em 6 de março de 2012.

o serviço é extremamente prejudicado. Isso não quer dizer que o usuário deveria poder utilizar uma capacidade de banda ilimitada, mas que a decisão sobre como melhor utilizar a banda contratada seja feita pelo usuário e não pelo provedor.

Por fim, provedores de acesso à Internet também têm um incentivo para bloquear conteúdos contrários aos seus interesses e que não estejam de acordo com a política de conteúdo escolhida por eles, ou ainda conteúdos que possam gerar responsabilidade.

Em um mercado competitivo, diversos problemas que o princípio da neutralidade de rede visa evitar não ocorreriam. Se um serviço não respeita a escolha do usuário e impõe limitações a seu acesso, a solução seria simplesmente contratar o serviço de outro provedor. Enquanto os usuários valorizarem a possibilidade de acessar conteúdos e aplicativos de sua escolha, um mercado competitivo naturalmente oferecerá tal serviço.

Historicamente, o mercado de telecomunicações foi considerado um monopólio natural.[50] Estudos do final do século XX, no entanto, mostraram como o monopólio na área de telefonia nos EUA podia ser explicado menos como consequência de uma característica natural do mercado e mais como o resultado de reiteradas ações do governo.[51]Apesar disso, o estudo elaborado pela Agência Nacional de Telecomunicações e apresentado no âmbito da consulta pública sobre o Plano Geral de Metas de Competição (PGMC) concluiu que, no mercado de infraestrutura e banda larga brasileiro, uma única empresa detém poder de mercado significativo em mais de 3.758 municípios.

Não obstante essa análise, há grande controvérsia sobre se um mercado competitivo de acesso à Internet seria suficiente para manter as características da Internet que o princípio da neutralidade de rede visa resguardar.[52] Van Schewick defende que a regulação é necessária mesmo nessa hipótese. Partindo do princípio *end to end*, que valoriza a Internet como uma ferramenta de múltiplos propósitos e agnóstica em relação a tecnologias específicas, ela identifica três características principais que permitiram que a Internet se tornasse a grande plataforma de inovação das últimas décadas: a) Inventores na rede sempre tiveram liberdade para criar quaisquer aplicativos que desejarem; da mesma forma, usuários sempre tiveram liberdade para escolher de forma independente quais aplicativos querem

---

[50] SPULBER, D.F. *Deregulating Telecommunications. Yale Journal of Regulation* 12(1), (1995): p. 25-67.

[51] Idem.

[52] Nesse sentido, veja VAN SCHEWICK, B. op. cit., YOO, C.S., op. cit., WU, T. Network Neutrality, Broadband Discrimination. *Journal of Telecommunications and High Technology Law*, v. 2, p. 141, 2003. Disponível em: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=388863>. Acesso em 15 de dezembro de 2011.

utilizar. b) O fato da rede ser de propósito geral (*application-blindness*) garantiu que provedores não pudessem interferir nessas escolhas, que eles não pudessem distorcer a competição entre aplicativos ou reduzir o lucro de desenvolvedores de aplicativos através de taxas de acesso. c) Finalmente, os baixos custos da inovação na Internet não só têm possibilitado o desenvolvimento de mais aplicativos, mas também permitem que um amplo e diverso grupo de pessoas inove, o que, por sua vez, aumenta a quantidade e a qualidade das inovações.[53]

A partir dessa análise, Van Schewick estabelece alguns critérios para avaliar normas de não discriminação que acreditamos ser muito úteis no processo de redação de uma regra de neutralidade de rede. São eles:

a) "Ela deve proteger os fatores que possibilitaram a **inovação de aplicativos** no passado para garantir que a Internet continue sendo uma plataforma para inovação e crescimento econômico no futuro;

b) Ela deve proteger os fatores que permitiram à Internet promover o **discurso democrático** e proporcionar um ambiente descentralizado para interação social e cultural no qual qualquer um pode participar;

c) Ela **não deve afetar a evolução da rede** além do que for necessário para atingir os objetivos da regulação da neutralidade de rede;

d) Ela deve tornar **simples** a tarefa de **determinar qual comportamento é permitido** e qual não o é, para garantir certeza aos participantes da indústria;

e) Ela deve manter os **custos de regulação baixos**."[54]

3.1 A regulação da neutralidade no cenário internacional

Nos últimos anos, governos e entidades reguladoras ao redor do mundo, despertados pelos cada vez mais frequentes exemplos de afronta à neutralidade de rede, iniciaram um processo de discussão e implementação das primeiras normas sobre neutralidade de rede. Seguindo a liderança do Chile, que em 2010 aprovou a primeira lei sobre neutralidade de rede do mundo, a Colômbia também adotou uma norma em seu plano nacional de desenvolvimento para im-

---

[53] VAN SCHEWICK, B. Opening Statement at the Federal Communications Commission's Workshop on Innovation. In: *Investment and the Open Internet in Cambridge, MA on January 13, 2010, WC Docket No. 07-52, GN Docket No. 09-191*. Disponível em: <http://cyberlaw.stanford.edu/publications/opening-statement-federal-communications-commission%E2%80%99s-workshop-innovation-investment>. Acesso em 5 de março de 2012.

[54] VAN SCHEWICK, B. *Network Neutrality: What a Non-Discrimination Rule Should Look Like*. Stanford Public Law Working Paper No. 1684677; Stanford Law and Economics Olin Working Paper No. 402 (September 20, 2010). Disponível em <http://ssrn.com/abstract=1684677>. Acesso em 22 de Novembro de 2012.

pedir práticas de discriminação de informações. No âmbito da União Europeia, a Holanda foi a pioneira na adoção de uma norma específica.

Nos EUA, a *Federal Communication Commission* (FCC) tem discutido e experimentado normas para garantir a neutralidade de rede desde o ano de 2005.[55] Após diversas consultas públicas, debates nos jornais e reuniões a portas fechadas com representantes da indústria, o órgão finalmente enviou para publicação as normas que visam garantir a neutralidade da rede naquele país e, em novembro de 2011, elas entraram em vigor.[56] As regras básicas do FCC sobre neutralidade de rede consistem em:

a) Transparência. Provedores de serviços de banda larga fixa e móvel devem divulgar suas práticas de gerenciamento de rede, características de *performance* e os termos e condições de seus serviços de banda larga;

b) Proibição de bloqueio. Provedores de serviço de banda larga fixa não podem bloquear conteúdo, aplicativos e serviços lícitos, nem mesmo aparelhos que não prejudiquem o funcionamento da rede; provedores de serviços de banda larga móvel não podem bloquear *websites* lícitos, nem mesmo bloquear aplicativos que compitam com seus serviços de voz ou vídeochamada; e

c) Proibição de discriminação de conteúdo de forma não razoável. Provedores de serviço de banda larga não podem discriminar de maneira não razoável o tráfego lícito de rede.

Para os defensores do princípio da neutralidade de rede, as regras ainda são tímidas. Primeiro, porque sua aplicação aos serviços de banda larga móvel é restrita, englobando tão somente a proibição do bloqueio de serviços que compitam com serviços específicos das operadoras dos serviços móveis. Segundo, porque ainda há margem para discriminação, desde que a mesma seja "razoável". A vagueza e indefinição sobre o que consistiria uma discriminação "não razoável" podem dar margem a alguns abusos que consumirão tempo e recursos do FCC para monitorá-los de perto.

É interessante notar que a proposta de regulamentação da neutralidade de rede nos EUA teve forte influência sobre as propostas e legislações referentes ao tema na América Latina. Para ilustrar esse ponto, incluímos abaixo um quadro mapeando como os principais elementos constantes nas normas de neutralidade do FCC estão presentes nas diversas legislações latino-americanas analisadas.

---

[55] ESTADOS UNIDOS. Federal Communications Commission. Policy Statement FCC 05-151. Disponível em: <http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-260435A1.pdf>. Acesso em 13 de julho de 2012.

[56] ESTADOS UNIDOS. Federal Communications Commission. Resolução FCC 10-201. Disponível em: <http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-10-201A1.pdf>. Acesso em 18 de julho de 2012.

QUADRO COMPARATIVO DAS LIBERDADES BÁSICAS PARA OPEN INTERNET DO FCC COM AS LEGISLAÇÕES E PROPOSTAS LEGISLATIVAS DO CHILE, ARGENTINA, COLÔMBIA, BRASIL, MÉXICO E VENEZUELA

Liberdades Básicas para Neutralidade de rede do FCC	Chile	Argentina	Colômbia	Brasil	México	Venezuela
Liberdade de acesso a qualquer conteúdo legal	Art. 24, H, a)	PL 1159-D-2011 Art. 1, a) PL S-1491/11 Art. 1	Lei 1.450 de 2011, Art. 56, 1.	Anteprojeto de Lei – Marco Civil da Internet Art. 10, *caput* Regulamento Anatel, Art. 59, *caput*	PL para modificação da Lei Federal de Telecomunicações Art. 44	Não há [56]
Liberdade para rodar qualquer aplicativo lícito [57]	Art. 24, H, a)	PL 1159-D-2011 Art. 1, a) PL S-1491/11 Art. 1	Lei 1.450 de 2011, Art. 56, 1.	Anteprojeto de Lei – Marco Civil da Internet Art. 10, *caput* Regulamento Anatel, Art. 59, *caput*	PL para modificação da Lei Federal de Telecomunicações Art. 44	Não há

[57] Vide próxima nota.

continuação >

QUADRO COMPARATIVO DAS LIBERDADES BÁSICAS PARA OPEN INTERNET DO FCC COM AS LEGISLAÇÕES E PROPOSTAS LEGISLATIVAS DO CHILE, ARGENTINA, COLÔMBIA, BRASIL, MÉXICO E VENEZUELA

Liberdades Básicas para Neutralidade de rede do FCC	**Chile**	**Argentina**	**Colômbia**	**Brasil**	**México**	**Venezuela**
Liberdade para conectar quaisquer dispositivos que não interfiram com o funcionamento da rede (carterfone)	Art. 24, H, b)	PL 1159-D-2011 Art. 1, b)	Lei 1.450 de 2011, Art. 56, 2.	Não consta na norma específica de neutralidade [57] Não consta na norma específica de neutralidade	Não consta na norma específica de neutralidade	Não há
Acesso a informações abrangentes sobre planos de serviço (transparência) [58]	Art. 24, H, d)	PL S-1491/11 Art. 2	Lei 1.450 de 2011, Art. 56, 4	Anteprojeto de Lei – Marco Civil da Internet Art. 8, IV Regulamento Anatel, Art. 59, §2º	Não consta na norma específica de neutralidade	Não há

[58] O fato desta liberdade não constar na norma específica de neutralidade não quer dizer que ela não esteja prevista em outra norma.

continuação >

QUADRO COMPARATIVO DAS LIBERDADES BÁSICAS PARA OPEN INTERNET DO FCC COM AS LEGISLAÇÕES E PROPOSTAS LEGISLATIVAS DO CHILE, ARGENTINA, COLÔMBIA, BRASIL, MÉXICO E VENEZUELA

Liberdades Básicas para Neutralidade de rede do FCC	**Chile**	**Argentina**	**Colômbia**	**Brasil**	**México**	**Venezuela**
Existe exceção ao princípio da neutralidade para fins de administração técnica ou de segurança?	Sim. Art. 24, H, a)	PL 1159-D-2011 Sim. Art. 1, c PL S-1491/11 Sim. Art. 3	Não	Sim. Art. 10, *caput* Sim. Art. 59, §2º	Não	Não se aplica
Existe a obrigação do oferecimento de serviço de controle parental pelos provedores a pedido dos usuários?	Sim. Art. 24, H, a)	PL 1159-D-2011 Sim. Art. 1, c[3] PL S-1491/11 Não	Sim. Art. 56, 3	Não Não	Não	Não se aplica

[59] O artigo em questão prevê a possibilidade de que o usuário peça ao provedor o bloqueio de conteúdos de sua escolha, o que pode ser interpretado como permitindo, dentre outros, o controle parental realizado pelo provedor.

3.2 Propostas de codificação da neutralidade de rede no Brasil

Na esteira da regulamentação global, duas propostas de regulação do princípio da neutralidade de rede surgiram no Brasil em 2011: o art. 10 do Marco Civil da Internet[60] e o art. 59 do Regulamento de Qualidade para Provedores de Serviço de Comunicação Multimídia[61], colocado em consulta pública pela Agência Nacional de Telecomunicações (Anatel).

A proposta do Marco Civil enviada ao Congresso Nacional em 2011, analisado ao longo do segundo capítulo dessa obra, disciplinou o princípio da neutralidade de rede da seguinte forma:

> *Art. 10. O responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma* ***isonômica*** *quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicativo, sendo* ***vedado estabelecer qualquer discriminação ou degradação do tráfego que não decorra de requisitos técnicos necessários à prestação adequada dos serviços****, conforme regulamentação da Agência Nacional de Telecomunicações – Anatel sobre preservação e garantia da neutralidade da rede.*

O *caput* do art. 10 estabelece uma vedação geral ao tratamento diferenciado de pacotes de dados na Internet por provedores. Esta vedação abarca tanto práticas de discriminação quanto de degradação. Ao fazer constar essas duas práticas, pretende-se vedar tanto o eventual bloqueio, quanto as práticas de administração de rede que priorizem determinadas aplicações ou conteúdos, em detrimento de outros. Aborda-se também, a proibição à prática de cobrança diferenciada pelos provedores de determinadas empresas, com base no tipo de aplicação ou conteúdo acessado por seus usuários. Com isso, pretende-se impedir que provedores distorçam a competição na rede ao aumentar as barreiras para entrada de novos competidores. A regra estabelecida se coaduna com o princípio *end to end* mencionado anteriormente e visa garantir a manutenção dos princípios elencados por Van Schewick.

É preciso reconhecer, contudo, que a implementação absoluta do princípio da neutralidade é impossível, e garantir um espaço de autonomia para a adminis-

---

[60] BRASIL. Projeto de Lei nº 2.126 de 2011, em tramitação na Câmara dos Deputados. Disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=517255>. Acessado em 18.07.2012.

[61] Anexo à Consulta Pública nº 45 da Agência Nacional de Telecomunicações. Disponível em: <http://sistemas.anatel.gov.br/SACP/Contribuicoes/TextoConsulta.asp?CodProcesso=C1514&Tipo=1&Opcao=>. Acessado em 18 de julho de 2012.

tração de tráfego, em função de certos requisitos técnicos, é crucial para permitir o funcionamento da rede. Uma regra absoluta proibiria, por exemplo, qualquer tentativa de impedir o envio de *spam* ou mesmo de evitar ataques de negação de serviço (DoS)[62], pois as contramedidas necessárias para impedir estes ataques requerem o bloqueio do acesso originado de determinados computadores. Tendo em vista a necessidade de criar exceções à regra geral da neutralidade optou-se, no Marco Civil, por delegar à Anatel o poder de regulamentar essas hipóteses.

Existem outras maneiras de permitir a flexibilização do princípio da neutralidade. A opção adotada na norma do *Federal Communications Commission* dos EUA, por exemplo, foi proibir a discriminação não razoável do tráfego na rede. O problema de uma norma como essa seria a ausência de critérios mais objetivos para auxiliar na definição de quais condutas deveriam ser consideradas exceções lícitas. Se tal norma fosse implementada, sua concretização dependeria exclusivamente do judiciário que, na ausência de conhecimento técnico necessário e sem outros critérios para basear suas decisões, poderia interpretá-la de maneira absolutamente diferente do objetivo que se quer alcançar.

Além da delegação da regulamentação a uma entidade com capacidade técnica para tanto, a proposta legislativa poderia ter adotado critérios adicionais para auxiliar o órgão regulador a estabelecer quais condutas deveriam constar nas exceções ao princípio da neutralidade.

O parágrafo único do art. 10 vai além do estabelecimento da neutralidade e também veda práticas de monitoramento, filtragem, análise ou fiscalização de tráfego na rede.

> *Parágrafo único. Na provisão de conexão à Internet, onerosa ou gratuita, é vedado monitorar, filtrar, analisar ou fiscalizar o conteúdo dos pacotes de dados, ressalvadas as hipóteses admitidas em lei.*

Além de reforçar a proibição ao bloqueio de conteúdos na rede, houve uma preocupação adicional em evitar a prática conhecida como *deep packet inspection*, que consiste na análise do conteúdo dos pacotes que trafegam pela rede por intermediários que deveriam somente transmiti-los.[63] Esta prática tornou-se alvo

---

[62] Para uma explicação simplificada de um ataque de negação de serviço veja: <http://pt.wikipedia.org/wiki/Ataque_de_nega%C3%A7%C3%A3o_de_servi%C3%A7o>. Acessado em 1º de julho de 2012.

[63] Para uma visão geral da tecnologia veja: <http://en.wikipedia.org/wiki/Deep_packet_inspection>. Acessado em 20 de julho de 2012.

de críticas quando uma empresa norte-americana começou a fazer acordos com provedores de acesso à Internet para monitorar o que seus usuários acessavam e oferecer propaganda a eles com base em seu histórico de acesso.[64] Isso, contudo, não implica em uma vedação absoluta às práticas de monitoramento de dados na rede e a exceção prevista ao fim do parágrafo já encontra, por exemplo, uma hipótese de aplicação nos parágrafos 2º e 3º do art. 13 do Marco Civil da Internet.[65]

A outra iniciativa de codificação do princípio da neutralidade de rede no Brasil encontra-se na consulta pública nº 45, realizada pela Anatel, que abordou o tema da seguinte maneira:

> *Art. 59. É vedado à prestadora realizar bloqueio ou tratamento discriminatório de qualquer tipo de tráfego, como voz, dados ou vídeo, independentemente da tecnologia utilizada.*
>
> *§ 1º A vedação prevista no caput desse artigo não impede a adoção de medidas de bloqueio ou gerenciamento de tráfego que se mostrarem* ***indispensáveis à garantia da segurança*** *e da* ***estabilidade do serviço*** *e das redes que lhe dão suporte;*
>
> *§ 2º Os critérios para bloqueio ou gerenciamento de tráfego de que trata o § 2º desse artigo devem ser informados previamente a todos os assinantes e amplamente divulgados a todos os interessados, inclusive por meio de publicação no sítio da prestadora na Internet;*
>
> *§ 3º O bloqueio ou gerenciamento de tráfego deve respeitar a privacidade dos assinantes, o sigilo das comunicações e a livre, ampla e justa competição.*

A proposta da Anatel assemelha-se ao do Marco Civil na proibição geral à discriminação. Contudo, a regra encontra vantagens sobre a outra proposta por alguns motivos. Primeiro, ela delineia melhor quais exceções ao princípio da neutralidade são permitidas (ou seja, somente aquelas relacionadas à **garantia da segurança** e da **estabilidade do serviço**). Ao especificar, ele restringe as exceções e reforça a aplicação do princípio geral. Além disso, o regulamento

---

[64] Para um resumo da polêmica envolvendo as práticas de monitoramento desenvolvidas pela empresa Phorm, veja: <http://en.wikipedia.org/wiki/Phorm>. Acessado em 20 de julho de 2012.

[65] BRASIL. Projeto de Lei nº 2.126/2011. Art. 13. Na provisão de aplicações de Internet é facultado guardar os registros de acesso dos usuários, respeitado o disposto no art. 7º.[...]
§2º Ordem judicial poderá obrigar, por tempo certo, a guarda de registros de acesso a aplicações de Internet, desde que se tratem de registros relativos a fatos específicos em período determinado, ficando o fornecimento das informações submetido ao disposto na Seção IV deste capítulo.
§3º Observado o disposto no §2º, a autoridade policial ou administrativa poderá requerer cautelarmente a guarda dos registros de aplicações de Internet, observados o procedimento e os prazos previstos nos §§ 3º e 4º do art. 11.

estabelece um requisito mais rigoroso que o do Marco Civil para que a exceção seja possível. Enquanto nele é proibida a "discriminação ou degradação do tráfego que não decorra de requisitos técnicos **necessários** à prestação adequada dos serviços**"**, o critério do regulamento é o da **indispensabilidade** que, ainda assim, se refere a hipóteses mais restritas.

Além disso, o regulamento de qualidade prevê uma obrigação de transparência sobre as eventuais hipóteses de discriminação adotadas, prática que é crucial para que consumidores possam corretamente comparar os serviços que lhe são oferecidos por diferentes provedores de Internet e tomar decisões informadas.

Por fim, vale lembrar que enquanto a norma geral do Marco Civil se aplicaria a qualquer tipo de acesso à Internet, o regulamento da Anatel abrangeria tão somente os prestadores do serviço de comunicação multimídia (SCM), ou seja, provedores de Internet. O acesso à Internet através da telefonia móvel não seria abarcado pela obrigação de neutralidade do regulamento.

Apesar dessas críticas, as propostas são um importante avanço na defesa da neutralidade de rede e na garantia da manutenção das características técnicas originais da Internet.

4

Privacidade

O ano de 2011 foi significativo para os debates envolvendo a proteção da privacidade e dos dados pessoais no ambiente digital. No Brasil, duas propostas regulatórias importantes merecem destaque: o Marco Civil da Internet e o Anteprojeto de Lei de Proteção a Dados Pessoais, levado a debate público por meio de procedimento inspirado no Marco Civil. Além disso, foi aprovada a Lei sobre Acesso à Informação mantida por órgãos públicos e entidades privadas sem fins lucrativos que tenham recebido recursos públicos. Essa lei é importante pelo uso estratégico que a Internet passa a ter no exercício do direito constitucional de acesso à informação.

4.1 Privacidade e dados pessoais

O desenvolvimento das tecnologias da informação, sobretudo da Internet, trouxe inegáveis benefícios à sociedade, como a facilidade e a rapidez na comunicação. Por outro lado, o progresso científico também ensejou o surgimento de novas formas de violação da privacidade alheia. Somado a isso, a própria Internet se revela um ambiente propício para a violação do direito à privacidade, na medida em que a maioria dos usuários ignora os diversos meios pelos quais seus dados pessoais são coletados e utilizados ao navegarem na rede.

Considerando o contexto brevemente narrado acima, a noção de privacidade e sua proteção não poderiam deixar de evoluir. Abandonando a clássica visão de um "direito a estar só", de cunho individualista e preocupado em estabelecer

um limite à intromissão do Estado na vida das pessoas, a concepção atual de privacidade se relaciona à necessidade de um maior controle na utilização das informações pessoais. Desse modo, o direito à privacidade assume a importante função de proteção dos dados pessoais, ao permitir o controle sobre as inúmeras possibilidades de seu tratamento (coleta, armazenamento e utilização). Esse controle serve para resguardar não somente os titulares dos dados, mas também a sociedade na qual os indivíduos se inserem, uma vez que tais dados podem revelar informações sensíveis (raça, opções políticas, religiosas, sexuais, etc.), as quais tem um potencial discriminatório.

O Brasil prevê proteção constitucional à privacidade no art. 5º, inciso X, que tutela a intimidade e a vida privada, e inciso XII, que garante a inviolabilidade da correspondência, do domicílio e das comunicações. A Constituição também assegura, no inciso LXXII do mesmo artigo, o direito de acesso do indivíduo às informações que lhe digam respeito e constem de registros ou bancos de dados de entidades governamentais ou de caráter público, bem como a possibilidade de retificação desses dados. Trata-se do remédio constitucional *habeas data*, disciplinado na lei 9.507, de 12 de novembro de 1997. Também o Código Civil trata da privacidade, ao estabelecer a inviolabilidade da vida privada no capítulo dedicado aos direitos da personalidade (art. 21).

Ao contrário de outros países, incluindo os vizinhos Argentina e Uruguai, o Brasil ainda não possui uma norma geral que trate da proteção dos dados pessoais. Um anteprojeto de lei sobre a matéria foi levado a discussão pública em 2011, como será explicado adiante. A única norma que trata especificamente da proteção de dados pessoais, além da lei que regulamenta a ação de *habeas data*, é o Código de Defesa do Consumidor, que, em seus artigos 43 e 44, regula a manutenção de bancos de dados e cadastros de consumidores, estabelecendo uma série de garantias a estes últimos.[66]

[66] Vale citar também a Lei Complementar 105, de 10 de janeiro de 2001, que dispõe sobre o sigilo das operações de instituições financeiras e traz, no parágrafo 3ª de seu artigo 1ª, algumas regras que geram repercussão na proteção de dados pessoais.

4.2 Iniciativas e propostas regulatórias com repercussão no tema da privacidade no Brasil

4.2.1 Anteprojeto de lei de dados pessoais

Em 2011 foi finalizado o debate público da proposta de um marco normativo para a proteção da privacidade e dos dados pessoais. O anteprojeto de lei foi fruto de uma parceria do Ministério da Justiça com o Observatório Brasileiro de Políticas Digitais, tendo como objetivo precípuo assegurar ao cidadão o controle e a titularidade sobre as suas próprias informações pessoais, o que concretizaria o direito constitucional à privacidade. O debate teve início em 30 de novembro de 2010 e se estendeu até 30 de abril de 2011.

O anteprojeto tem importância para as políticas digitais em pelo menos três aspectos, que serão abordados a seguir.

4.2.1.1 Vazamento de dados

Um dos principais desafios (e preocupações) provocados pela facilidade de se registrar informações de grande volume é a possibilidade de seu "vazamento" ou difusão indevida. No caso dos dados pessoais, o seu uso é cada vez mais frequente e necessário para o desempenho de atividades pelos setores público e privado. A ausência de uma política de administração dessas informações faz com que a sua manipulação ocorra de modo descuidado e em quantidades excessivas, o que facilita a sua difusão pública, acidental ou mesmo intencional.

Casos de vazamento de dados têm se tornado comuns, inclusive no Brasil, e o seu conhecimento provoca, justificadamente, uma sensação de desconfiança por parte do cidadão e consumidor em relação à instituição que permitiu a difusão das informações. E, mesmo que não se torne público, o vazamento de dados é capaz de provocar danos concretos em diversas ocasiões. Além disso, constitui um desafio técnico e organizacional para as corporações que tratam esses dados. Não é por outra razão que vem sendo objeto de crescente e intensa regulação no exterior, como será visto adiante.

O anteprojeto de lei sobre dados pessoais também trata da questão, ao obrigar que o tratamento de informações seja feito de modo a reduzir ao mínimo o risco de acesso não autorizado a esses dados (art. 23). Desse modo, o responsável pelo tratamento deve utilizar as medidas técnicas e administrativas proporcionais ao atu-

al estado da tecnologia, à natureza dos dados e às características específicas do tratamento, de modo a evitar, entre outros danos, a difusão, acidental ou ilícita, ou o acesso não autorizado a informações pessoais (princípio da segurança física e lógica – art. 8º, inciso VII). Ademais, tais medidas, sempre que possível, devem ser capazes de prevenir a ocorrência desses danos (princípio da prevenção – inciso X, art. 8º).

O tratamento de dados pessoais é considerado atividade de risco pelo anteprojeto. Isso significa que, em caso de vazamento de dados pessoais ou de qualquer outro dano patrimonial, moral, individual ou coletivo, responderá quem fez o tratamento de modo objetivo (art. 6º).

4.2.1.2 Tratamento de dados sensíveis

Outro tema controverso e preocupante envolve o tratamento de dados sensíveis, assim considerados aqueles dados pessoais que, pela sua natureza, podem ensejar discriminação para o seu titular. O anteprojeto coloca como exemplos de dados sensíveis aqueles relacionados à origem étnica ou racial, as convicções religiosas, filosóficas ou morais, as opiniões políticas, a filiação a sindicatos, partidos ou organizações religiosas, filosófica ou políticas, além dos dados de saúde, genéticos, biométricos e os referentes à vida sexual do indivíduo (art. 4º, inciso IV).

É possível visualizar a importância que os dados sensíveis possuem no desempenho de algumas atividades no âmbito digital, constituindo, em alguns casos, inclusive, o próprio cerne da atividade exercida. Assim ocorre com as redes sociais, que dependem da manipulação constante de dados pessoais, muitos dos quais sensíveis, e da sua alimentação pelos próprios usuários do serviço.

O anteprojeto dedica um capítulo à regulamentação do tratamento de dados sensíveis. Já de início, veda o fornecimento obrigatório desses dados (art. 21) e proíbe a formação de bancos com informações que revelem, de forma direta ou indireta, dados dessa natureza, salvo se houver disposição legal expressa. O anteprojeto, contudo, lista algumas situações em que o tratamento de dados sensíveis será permitido, como em caso de prévio consentimento do seu titular e quando for indispensável para o exercício de atribuições legais ou estatutárias de quem realiza a sua utilização (parágrafo 1º, inciso I), se para finalidade de pesquisa (inciso IV) ou se envolver dados manifestamente tornados públicos pelo seu titular (inciso V). Por outro lado, será considerado ilegal qualquer tratamento de dados sensíveis que seja utilizado para fins discriminatórios ao seu titular (parágrafo 2º do art. 21).

4.2.1.3 Publicidade comportamental

Outra atividade que envolve o tratamento de dados pessoais na Internet e pode ter repercussões negativas para a proteção da privacidade dos consumidores é a publicidade comportamental. Essa forma de publicidade, que envolve, por exemplo, a disposição de anúncios na página da conta de *e-mail* do usuário conforme seus hábitos e interesses, pode ser útil, mas também extremamente incômoda para quem a recebe. Além disso, essa prática pode ser considerada uma invasão de privacidade, na medida em que se baseia no levantamento de informações na correspondência pessoal, no caso do *e-mail*, do usuário.

A respeito do assunto, o anteprojeto prevê que os dados pessoais somente podem ser tratados após prévio consentimento do seu titular e desde que esse consentimento seja livre, expresso e informado (art. 9º). Além disso, conforme um dos princípios fundamentais do Anteprojeto, o tratamento deverá ser obrigatoriamente orientado pelas finalidades que motivaram a coleta dos dados e foram informadas ao seu titular. O tratamento estará adstrito às finalidades "determinadas, explícitas e legítimas" do responsável pela utilização dos dados (art. 8º, inciso I). Desse modo, estaria vedada a prática de propaganda comportamental que envolva determinado tratamento para o qual não foi obtido consentimento do titular dos dados.

Em caso de utilização de dados sensíveis, deverão ser observados também os dispositivos específicos sobre tais dados, já mencionados no item anterior.

4.2.2 A privacidade no Marco Civil da Internet

Outra proposta normativa de visível importância para as políticas digitais no país é o Anteprojeto de Lei chamado Marco Civil da Internet. Ao estabelecer princípios, garantias, direitos e deveres para uso da Internet no país, o Marco Civil prevê a proteção da privacidade e dos dados pessoais, o que se torna mais concreto na garantia do usuário ao ter definido no contrato de prestação de serviços de Internet o regime de proteção de seus dados pessoais, registros de conexão e registros de acesso a aplicações de Internet (art. 7°, inciso IV).

Uma das problemáticas que envolvem o tema é diretamente abordada pelo Marco Civil e diz respeito à guarda e disponibilização de registros de conexão[67] e de

[67] Compõem o conjunto de informações referentes à data e hora de início e término de uma conexão à Internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados (art. 5º, inciso VI).

acesso[68] a aplicações de Internet. Pela possibilidade de revelarem informações pessoais, o projeto de lei obriga que a guarda e a disponibilização desses registros ocorra de modo a preserver a intimidade, a vida privada, a honra e a imagem das partes direta ou indiretamente envolvidas (art. 10).

Na parte geral sobre guarda de registros, o anteprojeto determina que o provedor responsável pela guarda somente será obrigado a disponibilizar as informações que levem à identificação do usuário mediante autorização judicial (art. 10, parágrafo 1º). Em caso de violação do dever de sigilo estabelecido no Marco Civil, o infrator ficará sujeito a sanções de natureza civil, criminal e administrativas.

Em relação aos registros de conexão à Internet, o administrador do sistema autônomo[69] deverá manter tais registros sob sigilo, em ambiente controlado e de segurança, pelo prazo de um ano. O prazo de manutenção dos registros poderá ser superior mediante requisição cautelar de autoridade judicial ou administrativa (art. 11, *caput* e parágrafo 2°). Por outro lado, fica vedado o armazenamento de registros de acesso no caso de provisão de conexão, seja onerosa ou gratuita (art. 12). Tais registros de acesso poderão, a cargo do provedor de aplicações de Internet, ser guardados ou não, respeitados os direitos do usuário, previstos no art. 7°. A guarda desses registros poderá ser obrigatória, em razão de ordem judicial, caso se relacionem a fatos específicos em periodo determinado (art. 12, parágrafo 2°).

4.2.3 Lei de acesso à informação pública

O acesso à informação pública é hoje compreendido como um dos fundamentos para a consolidação da democracia. A premissa é que um cidadão bem informado passa a ter mais condições não só de conhecer os seus direitos essenciais, como a saúde, a educação e benefícios sociais, mas também de participar de modo efetivo da tomada de decisões que poderão afetá-lo (CGU, 2011).

Diversos organismos internacionais, incluindo a Organização das Nações Unidas e a Organização dos Estados Americanos, reconhecem o acesso à informação

[68] O conjunto de informações referentes à data e hora de uso de uma determinada aplicação de Internet a partir de um determinado endereço IP (art. 5º, inciso VIII).

[69] Trata-se da "pessoa física ou jurídica que administra blocos de endereço Internet Protocol – IP específicos e o respectivo sistema autônomo de roteamento, devidamente cadastrada no ente nacional responsável pelo registro e distribuição de endereços IP geograficamente referentes ao País" (art. 5º, inciso III).

como um direito fundamental. Na mesma linha, cerca de 90 países hoje adotam legislações específicas sobre o tema.

No Brasil, a lei nº 12.527, de 18 de novembro de 2011, passou a regulamentar o direito de acesso à informação, que já era previsto constitucionalmente (artigos 5º, inciso XXXIII; 37º, inciso II, §3º; 216º, §2°, da Constituição Federal).

A lei 12.527/2011 se apoia na noção de que a informação produzida, guardada, organizada e gerenciada pelo Estado em nome da sociedade é um bem público. Há então uma mudança de paradigma em matéria de transparência pública, ao se estabelecer que o acesso é a regra, e o sigilo, a exceção (CGU, 2011). Qualquer cidadão poderá, portanto, solicitar acesso às informações públicas, desde que não classificadas como sigilosas, conforme procedimento que será abordado adiante.

Submetem-se aos procedimentos dessa lei os órgãos e entidades públicas dos três Poderes (Executivo, Legislativo e Judiciário), de todos os níveis de governo (federal, estadual, distrital e municipal), assim como os Tribunais de Contas e o Ministério Público, bem como autarquais, fundações públicas, empresas públicas, sociedades de economia mista e demais entidades controladas direta ou indiretamente pela União, estados, Distrito Federal e município (art. 1º). A lei também se aplica a entidades privadas sem fins lucrativos que tenham recebido recursos públicos para a realização de ações de interesse público (art. 2º).

A lei é uma importante contribuição para as políticas digitais, na medida em que visualiza o potencial dos meios de comunicação viabilizados pela tecnologia da informação na efetivação do direito de acesso à informação (art. 3°, inciso III). Além disso, prevê o exercício da transparência ativa ao obrigar órgãos e entidades públicos a divulgarem, em local de fácil acesso, as informações de interesse coletivo ou geral que produziram ou custodiaram, o que inclui *sites* da Internet (parágrafo 2º). Entre as informações a serem disponibilizadas estão endereços e telefones das unidades e horários de atendimento ao público; dados gerais para acompanhamento de programas, ações, projetos e obras; e respostas a perguntas mais frequentes da sociedade.

Para os pedidos de acesso feitos pelos cidadãos, a lei estabelece prazos para o repasse das informações ao requerente: a resposta deve ser dada imediatamente, se estiver disponível, ou em até 20 dias, prorrogáveis por mais 10 dias. O pedido não precisa ser justificado, sendo obrigatório apenas conter a identificação do requerente e a especificação da informação solicitada. O requerente poderá recorrer no caso de indeferimento do pedido de acesso ou de negativa de acesso (art. 15º).

Há, contudo, exceções à regra de acesso no caso de dados pessoais e informações classificadas pelas autoridades como sigilosas.

A respeito das informações pessoais, consideradas aquelas relativas "à pessoa natural identificada ou identificável" (art. 4º, IV), a lei prevê que o seu tratamento deve ser feito de modo transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas (art. 31º). Essas informações dependem de consentimento expresso do seu titular ou de previsão legal para que possam ser divulgadas a terceiros. Contudo, será possível obter acesso à informação pessoal sem a exigência de prévio consentimento do seu titular nos casos em que o acesso a tais informações for necessário para: a) prevenção e diagnóstico médico, quando a pessoa for física ou legalmente incapaz, e para utilização no tratamento médico; b) realização de estatísticas e pesquisas científicas de interesse público ou geral, sendo vedada a identificação do titular das informações; c) cumprimento de ordem judicial; d) defesa de direitos humanos; e e) proteção do interesse público e geral preponderante.

As demais informações de acesso restrito são aquelas consideradas sigilosas. A regra geral é que uma informação pública somente poderá ser classificada como sigilosa se considerada imprescindível à segurança da sociedade (à vida, segurança ou saúde da população) ou do Estado (soberania nacional, relações internacionais, atividades de inteligência).

As informações públicas poderão ser classificadas como: I) ultrassecretas, com prazo de segredo de 25 anos, renovável uma vez; II) secretas, com prazo de segredo de 15 anos; e III) reservadas, com prazo de segredo de 5 anos (art. 24º).

A lei especifica as autoridades com prerrogativa de classificar as informações nos diferentes graus de sigilo. Quanto mais estrito o sigilo, maior o nível hierárquico do agente público (art. 27º). No entanto, não poderão ter acesso restrito às informações ou documentos que versem sobre condutas que impliquem em violação dos direitos humanos praticadas por agentes públicos ou a mando de autoridades públicas (art. 21º).

4.3 Iniciativas e propostas regulatórias com repercussão no tema da privacidade no âmbito internacional

4.3.1 Normas sobre proteção de dados pessoais

Em 2011, alguns países aprovaram normas que dispõem sobre a proteção de dados pessoais, o que, evidentemente, terá impacto no tratamento desses dados na Internet. O Peru se junta ao grupo dos países latino-americanos, incluindo Chile, Argentina, Uruguai, México e Colômbia, a adotar uma legislação específica sobre o tema, tendo como inspiração a experiência normativa europeia. A *Ley de Protección de Datos Personales* (*Ley Nº 29.733*) foi apresentada pela presidência a fim de adequar o Peru aos acordos de livre comércio que possui com Estados Unidos e Canadá e o futuro acordo com a União Europeia.[70]

No contexto asiático, duas iniciativas importantes foram adotadas. Em abril de 2011, a Índia adotou novas regras sobre privacidade, conhecidas como *Information Technology Rules*. Essas regras impõem uma série de obrigações às corporações que promovam o tratamento de dados pessoais. Tais obrigações exigem que as corporações estabeleçam políticas de privacidade, restrinjam o processamento de dados sensíveis e a transferência internacional de dados, bem como a adoção de medidas adicionais de segurança. As novas regras apresentam similaridades com a legislação europeia sobre privacidade e a sua implementação é tida como um desafio para prestadores de serviço e consumidores.[71]

A China, a exemplo do Brasil, também não possui uma legislação uniforme sobre a proteção de dados pessoais. Contudo, em setembro de 2011, a província de Jiangsu publicou o Regulamento de Tecnologia da Informação, que inclui dispositivos sobre a coleta e o uso de dados pessoais e sanções em caso de violação a essas previsões. A China possui diversas normas sobre a proteção de informações pessoais, mas a maioria se dirige especificamente a determinadas áreas (comércio eletrônico ou bancos). O regulamento é visto como um importante marco rumo à adoção de uma lei nacional de proteção a dados pessoais pelo país.[72]

---

[70] Disponível em: <http://www.huntonprivacyblog.com/2011/08/articles/english-translation-of-perus-law-for-personal-data-protection-released/>. Acesso em 20 de julho de 2012.

[71] Disponível em: <http://www.huntonprivacyblog.com/2011/05/articles/india-drafts-new-privacy-regulations/>. Acesso em 20 de julho de 2012.

[72] Disponível em: <http://www.huntonprivacyblog.com/2011/11/articles/new-chinese-legislation-includes-provisions-protecting-personal-information/>. Acesso em 20 de julho de 2012.

5

A regulação da Internet na reforma da Lei de Direitos Autorais: o Artigo 105-A da proposta

Após um longo processo de audiências, seminários e reuniões iniciado em 2007, envolvendo diversos setores da sociedade, o Ministério da Cultura, sob a gestão de João Luiz Silva Ferreira (Juca Ferreira), elaborou um anteprojeto de lei para a reforma da Lei de Direitos Autorais (LDA – Lei nº 9.610, de 1998), levado à consulta pública em junho de 2010.

Ciente do descompasso da lei atual e de toda sua problemática, a gestão de Juca Ferreira, segundo o governo Lula e em consonância com a gestão anterior, de Gilberto Gil, pretendeu, através da revisão da lei, constituir um instrumento para desenvolver e consolidar a economia da cultura no país, garantindo, ao mesmo tempo, os direitos constitucionais dos autores e da sociedade de ter acesso à educação, à informação e à cultura. Historicamente, é a primeira vez que adotamos uma atitude progressista voltada para a regulação dos direitos autorais.

Ao longo da consulta pública, o Ministério da Cultura apresentou justificativas e esclarecimentos bastante elucidativos, permitindo que a sociedade entendesse a exata intenção do governo com a reforma da lei. Entre os principais objetivos da proposta, encontram-se: ampliar e assegurar efetivo estímulo e proteção aos autores e às suas criações; promover o equilíbrio de direitos entre todos envolvidos; ampliar e democratizar o acesso da população aos bens e serviços culturais; sintonizar a legislação com os novos paradigmas estabelecidos pelo ambiente digital; e viabilizar a atuação do Estado na formulação de políticas públicas de

promoção, supervisão, regulação e defesa dos interesses da sociedade e do país no âmbito interno e nos fóruns internacionais.[73]

Em janeiro de 2011, Ana Buarque de Hollanda assumiu o Ministério da Cultura e, em função da mudança na gestão, o Anteprojeto de revisão da Lei de Direito Autoral retornou da Casa Civil para o Ministério da Cultura. Durante o período de análise do texto pela Ministra da Cultura e pela Diretoria de Direitos Intelectuais da Secretaria de Políticas Culturais, optou-se por novas alterações e por abrir novamente o texto para consulta[74].

O processo de consulta ocorreu entre os dias 25 de abril e 30 de maio de 2011, desta vez de forma menos democrática e menos transparente, permitindo comentários apenas sobre alguns temas e somente por especialistas. Terminada essa etapa de elaboração da proposta final do anteprojeto de lei, houve o encaminhamento de volta à Casa Civil, onde o projeto se encontra para análise e posterior envio ao Congresso Nacional.

Dentre as alterações, um trecho é de especial interesse no que diz respeito à regulação da Internet. O texto enviado à Casa Civil prevê, em seu art. 105-A, a responsabilização solidária de provedores de conteúdo que não tomarem as providências cabíveis para tornar indisponível o conteúdo apontado como infringente pelo titular dos direitos autorais. Dessa forma, o texto do artigo estabelece que:

> *Art. 105-A. Os provedores de aplicações de Internet poderão ser responsabilizados solidariamente, nos termos do art. 105, por danos decorrentes da colocação à disposição do público de obras e fonogramas por terceiros, sem autorização de seus titulares, se notificados pelo titular ofendido ou mandatário e não tomarem as providências para, no âmbito do seu serviço e dentro de prazo razoável, tornar indisponível o conteúdo apontado como infringente.*
>
> *§ 1º Os provedores de aplicações de Internet devem oferecer de forma ostensiva ao menos um canal eletrônico dedicado ao recebimento de notificações e contranotificações, sendo facultada a criação de mecanismo automatizado para atender aos procedimentos dispostos nesta Seção.*
>
> *§ 2º A notificação de que trata o caput deste artigo deverá conter, sob pena de invalidade:*

---

[73] Ver<http://www.cultura.gov.br/site/2010/04/12/nota-a-sociedade-sobre-a-revisao-da-lei-de-direito-autoral/>. Acesso em 15 de maio de 2010.

[74] As regras referentes à nova consulta podem ser encontradas no *site*: <http://www.cultura.gov.br/site/2011/04/20/ultima-fase-da-revisao-da-lda/>. Acesso em 3 de março de 2012.

I – identificação do notificante, incluindo seu nome completo, seus números de registro civil e fiscal e dados atuais para contato;

II – data e hora de envio;

III – identificação clara e específica do conteúdo apontado como infringente, que permita a localização inequívoca do material pelo notificado;

IV – descrição da relação entre o notificante e o conteúdo apontado como infringente; e

V – justificativa jurídica para a remoção.

§ 3º Ao tornar indisponível o acesso ao conteúdo, caberá aos provedores de aplicações de Internet informar o fato ao responsável pela colocação à disposição do público, comunicando-lhe o teor da notificação de remoção e fixando prazo razoável para a eliminação definitiva do conteúdo infringente.

§ 4º Caso o responsável pelo conteúdo infringente não seja identificável ou não possa ser localizado, e desde que presentes os requisitos de validade da notificação, cabe aos provedores de aplicações de Internet manter o bloqueio.

§ 5º É facultado ao responsável pela colocação à disposição do público, observados os requisitos do § 2º, contranotificar os provedores de aplicações de Internet, requerendo a manutenção do conteúdo e assumindo a responsabilidade exclusiva pelos eventuais danos causados a terceiros, caso em que caberá aos provedores de aplicações de Internet o dever de restabelecer o acesso ao conteúdo indisponibilizado e informar ao notificante o restabelecimento.

§ 6º Qualquer outra pessoa interessada, física ou jurídica, observados os requisitos do § 2º, poderá contranotificar os provedores de aplicações de Internet, assumindo a responsabilidade pela manutenção do conteúdo.

§ 7º Tanto o notificante quanto o contranotificante respondem, nos termos da lei, por informações falsas, errôneas e pelo abuso ou má-fé.

§ 8º Os usuários que detenham poderes de moderação sobre o conteúdo de terceiros se equiparam aos provedores de aplicações de Internet para efeitos do disposto neste artigo.

Em primeiro lugar, deve-se destacar que a proposta determina a remoção de conteúdos supostamente infringentes, independentemente da análise da procedência do pedido, seja pelo provedor, seja pelo Judiciário. Posto de outro modo, o dispositivo transfere para o titular o poder de decidir sobre a legalidade do uso da obra, o que pode causar alguns problemas. Isso ocorre porque a mera possibilidade de responsabilização do provedor já constitui incentivo suficiente para que o provedor acate, sem questionar, todas as ordens de remoção de conteúdo enviadas por titulares. O titular obviamente tem, por seu turno, um incentivo para notificar todo e qualquer uso não autorizado de sua obra.

Enquanto em alguns casos não restarão dúvidas sobre o caráter infringente do uso de determinada obra, outros tantos existirão em que somente a análise individual e contextualizada poderá determinar se o uso é ilegal ou não. Casos poderão existir, por exemplo, em que o uso consistirá em uma limitação ao direito do autor, previsto nos artigos 46 e seguintes da LDA, hipótese em que o uso independe de autorização do autor. Poderão também ocorrer casos em que a obra já esteja em domínio público e que a alocação de incentivos entre provedores, usuários e titulares acarretem na retirada de obras que, de outra forma, poderiam ser livremente e legalmente publicadas na Internet.[75] O dispositivo, da forma como se encontra, poderá dar ensejo ao uso abusivo do direito do autor, podendo restringir severamente alguns direitos, tais como o direito à liberdade de expressão e as exceções e limitações ao direito do autor.

Apesar do dispositivo legal, em seu parágrafo 5º – facultar ao responsável pela colocação à disposição do público a contranotificação dos provedores e a manutenção do conteúdo – é muito provável que este usuário, mesmo acreditando não haver ilegalidade em sua conduta, opte por não apresentar contranotificação pelo receio de ser responsabilizado e por ter que arcar com os dispendiosos custos de um processo judicial.[76]

Optando pela contranotificação, o usuário passa a assumir a responsabilidade exclusiva pelo conteúdo e por eventuais danos causados, enquanto o provedor de Internet, diante de uma eventual contranotificação, deve imediatamente republicar o conteúdo. Além disso, conforme o parágrafo 6º deste mesmo artigo, qualquer outra pessoa interessada pode contranotificar, desde que assuma responsabilidade por eventual infração autoral realizada pelo autor da publicação original.[77]

---

[75] Vale destacar que esta não é uma possibilidade remota, como alguns podem imaginar. Muito pelo contrário, como demonstrou o prof. Sérgio Branco em seu livro "O Domínio Público no Direito Autoral Brasileiro", já há diversos casos de arquivos públicos que simplesmente ignoram o domínio público, colocando restrições e cobrando pagamentos pelo uso de obras em domínio público.

[76] § 5º – É facultado ao responsável pela colocação à disposição do público, observados os requisitos do § 2º, contranotificar os provedores de aplicações de Internet, requerendo a manutenção do conteúdo e assumindo a responsabilidade exclusiva pelos eventuais danos causados a terceiros, caso em que caberá aos provedores de aplicações de Internet o dever de restabelecer o acesso ao conteúdo indisponibilizado e informar ao notificante o restabelecimento.

[77] § 6º – Qualquer outra pessoa interessada, física ou jurídica, observados os requisitos do § 2º, poderá contranotificar os provedores de aplicações de Internet, assumindo a responsabilidade pela manutenção do conteúdo.

Além disso, um dos objetivos da proposição do art. 105-A diz respeito justamente à harmonização do regime da Lei de Direitos Autorais com o proposto no Marco Civil da Internet. Ocorre que, após larga discussão no âmbito da consulta pública do Marco Civil da Internet, a redação final passou a exigir ordem judicial para remover qualquer conteúdo apontado como infringente. Dessa forma, a uniformização das propostas deveria caminhar no sentido de exigir ordem judicial para remoção do conteúdo supostamente infringente também no presente projeto.

Conforme debatido no âmbito do Marco Civil da Internet, a aprovação de um sistema que defina a responsabilidade dos intermediários por conteúdo postado por terceiros criaria um incentivo econômico para que estes promovam a remoção de conteúdo independentemente de uma avaliação do Poder Judiciário sobre a ilegalidade da informação apontada como infringente.

6

Governança da Internet

6.1 Governança da Internet no plano internacional

A governança da Internet refere-se aos processos segundo os quais emergem os consensos, princípios, normas de conduta e de tomada de decisão relacionados à Internet. Os objetivos principais do regime de governança da Internet são, por um lado, garantir o bom funcionamento da rede e, por outro, compartilhar informações e boas práticas de maneira a avançar rumo à harmonização e a compatibilização de políticas.

O regime de governança da Internet tem algumas características particulares que o distinguem de grande parte dos regimes internacionais: 1) é multissetorial, ou seja, dele participam, com relativa igualdade, vários atores, como governos, sociedade civil, setor privado, comunidade técnica e acadêmica; 2) a legitimidade dos participantes do regime advém sobretudo da sua *expertise* e de sua capacidade de contribuir no processo de elaboração de políticas; 3) os resultados dos processos de governança nem sempre se materializam em tratados ou acordos formais; autorregulação, *soft law*[78] e boas práticas tem um papel importante para o avanço do regime.

---

[78] Uma variedade de instrumentos se encontra sob o manto genérico da *soft law*. Recebem essa denominação tanto os tratados que incluem obrigações vagas ou fracas, que estabelecem metas gerais e programas de ação, como os instrumentos sem caráter obrigatório, como as resoluções e termos de conduta. Estes possuem caráter voluntário e podem ser formulados com a participação de atores governamentais e não governamentais. Chinkin, C. *The Challenge of soft law: development and change in international law*. *International and Compartive Law Quarterly*, vol 38. New York: *Cambridge University Press*, 1989, p. 851-2.

A governança da Internet pode ser exercida em vários níveis – nacional, regional e global –, que se influenciam mutuamente. As decisões tomadas no plano internacional, por exemplo, impactam e restringem as opções de regulação e de políticas que podem ser adotadas nacionalmente.

Os temas tratados nos fóruns internacionais dedicados à governança da Internet têm íntima relação com os interesses dos usuários da rede: neles há a discussão da privacidade, do acesso a conteúdos, da liberdade de expressão, da segurança e de estratégias para a ampliação do acesso e barateamento dos custos de conexão, dentre outros. Diante disso, o acompanhamento das discussões no âmbito internacional é de fundamental importância para que se possa influir nas futuras políticas de regulação da rede.

6.2 Um panorama da governança da Internet em 2011

Ao longo do ano de 2011, a governança da Internet tornou-se um tema extremamente politizado. Parece ter havido a superação definitiva do entendimento de que a governança da Internet é um tema exclusivamente técnico e de que se resume à gestão da infraestrutura e dos recursos críticos (nomes de domínio e números IP). O processo de politização do tema não é novo, mas acentuou-se bastante, principalmente diante das repercussões do *WikiLeaks* e da importância da Internet para o ativismo social, a exemplo do que aconteceu na Primavera Árabe.

Os exemplos que corroboram o aumento da importância do tema nas agendas políticas nacionais são abundantes: os seminários promovidos pelo Conselho da Europa, a conferência de Viena sobre Internet e Direitos Humanos, o Fórum sobre a Internet promovido pelo G8 antes da reunião de cúpula de Deauville e as discussões no âmbito do Fórum IBAS, que congrega Índia, Brasil e África do Sul. Concomitantemente, o tema expandiu-se para além dos Ministérios que lidam com comunicações e tecnologia, o que amplia os desafios para coordenar as políticas de governança da Internet no âmbito governamental.

As questões ligadas à cibersegurança e aos direitos humanos tiveram destaque. Vários incidentes, como vazamentos de informação, ações coordenadas de *hackers* e *crackers* e ataques DDoS impulsionaram a discussão sobre segurança nos meios de comunicação. Houve também esforços para que certos temas, como a proteção à propriedade intelectual *on-line*, tivessem destaque nas discussões sobre segurança, em um processo contínuo de recrudescimento do *enforcement*

e majoração das penalidades. Paralelamente, houve a intensificação das discussões acerca da liberdade de expressão e de associação na rede e sobre as possíveis implicações negativas das políticas de segurança sobre os direitos humanos, inclusive sobre a privacidade.

Consolida-se no âmbito internacional o entendimento de que é preciso desenvolver princípios norteadores para a governança da Internet, que irão servir de baliza à elaboração e harmonização de normas e de políticas públicas. Uma pluralidade de iniciativas para definição desses princípios foi trazida à tona, elaborada, dentre outros, pela OCDE, pelo Conselho da Europa e pela União Europeia. O mesmo entendimento prevaleceu no Brasil, no processo de elaboração do Marco Civil da Internet. Tanto o Marco Civil como os princípios para a Governança e uso da Internet no Brasil, elaborados pelo CGI.br, têm fornecido elementos para a discussão no plano internacional.

Tornou-se mais palpável também a tendência de privatização da governança da Internet, diante da fragmentação da rede em plataformas fechadas e operadas em regime privado, como as redes sociais. A convergência entre plataformas acentua esse quadro e deixa os usuários vulneráveis diante das decisões que são tomadas unilateralmente pelas empresas acerca de temas importantes, como as suas políticas de privacidade. Por outro lado, alguns atores privados, como os provedores de acesso e as entidades de registro de nomes de domínio, têm sido cada vez mais pressionados a atuar como vigilantes do comportamento dos usuários na rede e a agir como partícipes para coibir condutas reputadas ilícitas, em um processo de privatização e terceirização da aplicação da lei.

Em 2011, iniciou-se um processo de rediscussão de algumas das principais instituições relacionas à governança da Internet. A Assembleia Geral das Nações Unidas decidiu renovar o mandato do Fórum de Governança da Internet (IGF) até 2015, e um Grupo de Trabalho foi criado com o intuito de fazer sugestões para o aperfeiçoamento do Fórum. A ICANN (Corporação da Internet para Designação de Nomes e Números ou *Internet Corporation for Assigned Names and Numbers*) também passa por um processo de reforma administrativa e de escolha de um novo CEO. Encontra-se em curso ainda a implementação da controversa decisão de criar novos nomes de domínio genéricos de primeiro nível (*top level domain names* ou gTLDs).

Diante dessa combinação de fatores, é possível prever o maior interesse da sociedade sobre o tema da governança da Internet, sobretudo para garantir que

direitos já consagrados sejam respeitados na rede. Pode-se prever ainda o maior envolvimento dos governos nesse tema e uma possível tentativa de aprofundar o diálogo com os atores privados, sobretudo com as empresas.

6.3 Iniciativas voltadas à elaboração de princípios para a governança da Internet

Há um consenso emergente na cena internacional de que é importante desenvolver um quadro harmônico de princípios gerais antes de promover a regulação de temas específicos relacionados à Internet. Esse rol de princípios comuns ajudaria a promover a convergência entre os atores e balizaria normas internacionais. Fazendo um paralelo com os processos políticos que ocorrem no âmbito nacional, alguns chegam a afirmar que a Internet passa por um momento "constitucional", já que os princípios em discussão atualmente podem servir de base a todo o arcabouço normativo que se aplicará à sociedade em rede no futuro.[79]

6.3.1 Princípios do CGI.br para a governança e uso da Internet no Brasil

O Comitê Gestor da Internet – CGI.br é uma experiência pioneira e única. Composto por membros do governo, do setor empresarial, do terceiro setor e da comunidade acadêmica, o CGI.br representa um modelo de governança democrático e plural, em que os representantes de cada segmento não governamental são eleitos para compor um órgão colegiado que exerce o papel de coordenar e integrar as iniciativas de serviços de Internet no país.

O CGI.br também foi um dos pioneiros na discussão sobre princípios para a Internet. Em 2009, considerando a necessidade de lastrear suas ações e decisões em bases sólidas, o CGI.br aprovou os seguintes princípios para a governança e uso da Internet no Brasil:[80]

---

[79] IGF *workshop* 144: *Human Rights Come First: a Constitutional Moment for Internet Governance?* Nairobi, 2011. Disponível em: <http://www.intgovforum.org/cms/component/content/article/71-transcripts-/815-ig4d-workshop-144-human-rights-come-first-a-constitutional-moment-for-internet-governance>. Acesso em 20 de julho de 2012.

[80] CGI.br. Princípios da para a governança e uso da Internet no Brasil. RES/2009/003/P. Disponível em: <http://www.cgi.br/regulamentacao/resolucao2009-003.htm>. Acesso em 20 de julho de 2012.

1. Liberdade, privacidade e direitos humanos

O uso da Internet deve guiar-se pelos princípios de liberdade de expressão, de privacidade do indivíduo e de respeito aos direitos humanos, reconhecendo-os como fundamentais para a preservação de uma sociedade justa e democrática.

2. Governança democrática e colaborativa

A governança da Internet deve ser exercida de forma transparente, multilateral e democrática, com a participação dos vários setores da sociedade, preservando e estimulando o seu caráter de criação coletiva.

3. Universalidade

O acesso à Internet deve ser universal para que ela seja um meio para o desenvolvimento social e humano, contribuindo para a construção de uma sociedade inclusiva e não discriminatória em benefício de todos.

4. Diversidade

A diversidade cultural deve ser respeitada e preservada e sua expressão deve ser estimulada, sem a imposição de crenças, costumes ou valores.

5. Inovação

A governança da Internet deve promover a contínua evolução e ampla difusão de novas tecnologias e modelos de uso e acesso.

6. Neutralidade da rede

Filtragem ou privilégios de tráfego devem respeitar apenas critérios técnicos e éticos, não sendo admissíveis motivos políticos, comerciais, religiosos, culturais ou qualquer outra forma de discriminação ou favorecimento.

7. Inimputabilidade da rede

O combate a ilícitos na rede deve atingir os responsáveis finais e não os meios de acesso e transporte, sempre preservando os princípios maiores de defesa da liberdade, da privacidade e do respeito aos direitos humanos.

8. Funcionalidade, segurança e estabilidade

A estabilidade, a segurança e a funcionalidade globais da rede devem ser preservadas de forma ativa por meio de medidas técnicas compatíveis com os padrões internacionais e estímulo ao uso das boas práticas.

9. Padronização e interoperabilidade

A Internet deve basear-se em padrões abertos que permitam a interoperabilidade e a participação de todos em seu desenvolvimento.

10. Ambiente legal e regulatório

O ambiente legal e regulatório deve preservar a dinâmica da Internet como espaço de colaboração.

Esse rol de princípios foi apresentado aos participantes do IGF como uma contribuição brasileira à discussão sobre princípios no plano global, tendo obtido ampla aceitação. Markus Kummer, ex-secretário-executivo do IGF, opinou: "Eu poderia imaginar um consenso em torno destes princípios fundamentais. Ficaria feliz em apoiá-los". Vint Cerf acrescentou: "Estes são princípios que eu acho que podem ser amplamente aceitos".[81]

O documento elaborado pelo CGI.br foi um dos estímulos a iniciativas voltadas a elaboração de princípios surgidas desde então.

6.3.2 Princípios elaborados pelo Conselho da Europa (CoE)

O Conselho da Europa (CoE) é uma organização internacional que visa promover a cooperação entre países europeus para o fortalecimento dos direitos humanos, da democracia e do Estado de Direito. Foi fundada em 1949 e tem 47 Estados membros. Dentre os órgãos institucionais do CoE, há a Corte Europeia dos Direitos Humanos, responsável por aplicar a Convenção Europeia dos Direitos Humanos, e o Conselho de Ministros, que produz declarações e recomendações, de caráter não vinculante, mas com peso político significativo, característico dos instrumentos de *soft law*.

Em 2005, os Estados membros do CoE decidiram analisar a viabilidade de um instrumento legal que pudesse tratar dos fluxos transfronteiriços na Internet. Com esse objetivo, criou-se um grupo *ad hoc* de *experts* com composição multissetorial, que propôs dez princípios para a governança da Internet[82], endossados na declaração conjunta do Comitê de Ministros do CoE.[83] Além da ênfase dada à proteção dos direitos fundamentais, alguns princípios merecem destaque.

Primeiro, afirma-se que qualquer política aplicada à Internet deve reconhecer sua natureza global e respeitar o fluxo irrestrito do tráfego transfronteiriço na

---

[81] Transcrições da sessão *Taking stocks of Internet Governance and the way forward*. IGF 2010, Vilnius. Disponível em: <http://www.intgovforum.org/cms/component/content/article/102-transcripts2010/687-taking-stock>. Acesso em 20 de julho de 2012.

[82] *Council of Europe ad hoc Advisory Group on Cross-border* Internet. *Proposal for a draft Council of Europe Committee of Ministers Declaration on Internet Governance Principles*. Disponível em: <http://www.coe.int/t/dghl/standardsetting/media-dataprotection/conf-internet-freedom/Internet%20Governance%20Principles.pdf>. Acesso em 20 de julho de 2012.

[83] Conselho Europeu. *Declaration by the Committee of Ministers on Internet governance principles*. Adotado pelo Comitê de Ministros em 21 de setembro de 2011. Disponível em: <https://wcd.coe.int/ViewDoc.jsp?id=1835773>. Acesso em 20 de julho de 2012.

rede. Esse princípio geral é corroborado por outros, como o respeito à abertura, à interoperabilidade e à natureza "*end-to-end*" da Internet, além da promoção da neutralidade da rede.

Em segundo lugar, o documento se posiciona sobre temas importantes relacionados ao exercício de governança da Internet. Afirma-se que "o setor privado deve manter o seu papel de liderança em questões técnicas e operacionais", mas "tem o dever de assegurar a transparência e a prestação de contas à comunidade global em relação às ações que tem impacto sobre a política pública".

A característica multissetorial é apontada como fundamental para a perpetuação da estabilidade e da resiliência do funcionamento da Internet. A promoção do multissetorialismo pode ser encontrada em maior parte nas inciativas que buscam elencar princípios, mas é interessante perceber que os membros do grupo *ad hoc* do CoE se dedicaram à discussão de um tema atual e desafiador no âmbito teórico: a relação entre o sistema internacional, de caráter eminentemente intergovernamental, e o modelo multissetorial da governança da Internet. Segundo Wolfgang Kleinwächter, membro do grupo *ad hoc*, "nossa conclusão, no início dos trabalhos do grupo, foi a de que continuaremos a ter um sistema de tratados multilaterais. Mas os tratados multilaterais no futuro provavelmente vão se desenvolver dentro de um ambiente multissetorial. O princípio multissetorial seria um princípio geral e, a partir dessa abordagem, é possível chegar a direitos, deveres e responsabilidades específicos dos governos".[84]

Dessa forma, é possível prever uma relação de complementaridade entre *hard law* e *soft law* e de interdependência entre os grupos de atores. Ainda segundo Kleinwächter, a abordagem a partir da *soft law*, de caráter não vinculante, como no caso da declaração de princípios do CoE, tem a vantagem de permitir chegar rapidamente a um entendimento convergente. O documento significaria não um resultado final, mas um ponto de partida para uma discussão colaborativa e multissetorial.[85].

Paralelamente à discussão sobre princípios, o Comitê de Ministros do CoE alertou os Estados membros sobre ameaças à liberdade de expressão e de associa-

---

[84] Wolfgang Kleinwächter. Transcrições do *Workshop* 203 do IGF 2011. *Internet Governance Principles: Initiatives Toward the Improvement of a Global Internet Governance.* Nairobi, 2011. Disponível em: <http://www.intgovforum.org/cms/component/content/article/71-transcripts-/912-ig4d-workshop-203-internet-governance-principles-initiatives-toward-the-improvement-of-a-global-internet-governance>. Acesso em 20 de julho de 2012.

[85] Ibidem.

ção na Internet, que podem advir da pressão política atualmente exercida sobre os prestadores de serviços de Internet e sobre as plataformas *on-line* para que atuem como copartícipes no processo de aplicação das leis. O Comitê também expressou sua preocupação em relação ao cerceamento à liberdade de expressão causado por ataques a *websites* de mídia independente, a *sites* de vazamentos, como o *Wikileaks*, de defensores de direitos humanos e de dissidentes políticos. Foi aprovada uma declaração conjunta, na qual se destacou o importante papel desses atores como facilitadores do exercício dos direitos à liberdade de expressão e à liberdade de associação.[86]

6.3.3 A Comissão Europeia e o "Internet Compact"

A Comissão Europeia desenvolve políticas nos temas relacionados à Internet por meio da atuação da Diretoria Geral sobre Sociedade da Informação e Mídia, cuja competência abrange um amplo leque de temas, como infraestrutura e telecomunicações, governo eletrônico, educação *on-line*, conteúdo em formato digital, dentre outros. No âmbito da governança da Internet, a Comissão tem sido um ator importante, com participação ativa nos debate sobre arranjos institucionais.

Em 2011, durante o encontro de alto nível da OCDE sobre economia da Internet, a vice-presidente da Comissão Europeia, Neelie Kroes, ponderou que "A academia, o setor privado e a sociedade civil têm contribuído enormemente para o sucesso da Internet. Os políticos devem atentar para isso. Mas as autoridades públicas não podem nem devem permanecer em segundo plano. A Internet tem relevância e traz benefícios para os cidadãos, para a economia e para a sociedade. Por essa razão, é de interesse dos formuladores de políticas públicas. Um dos desafios é corresponder esse interesse legítimo sem prejudicar as características da Internet".[87]

Segundo a comissária, a Internet deveria permanecer, na medida do possível, livre de intervenções. A regulação deveria ser vista como última alternativa e o

---

[86] CONSELHO EUROPEU. *Declaration of the Committee of Ministers on the protection of freedom of expression and freedom of assembly and association with regard to privately operated Internet platforms and online service providers*. Adotada pelo Comitê de Ministros em 7 de dezembro de 2011. Disponível em: <https://wcd.coe.int/ViewDoc.jsp?id=1883671&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383>. Acesso em 20 de julho de 2012. Tradução para o português disponível em: <http://observatoriodainternet.br/conselho-da-europa-alerta-sobre-ameacas-a-liberdade-de-expressao-on-line>. Acesso em 20 de julho de 2012.

[87] KROES, Neelie. *OECD High Level Meeting on the Internet Economy*. Paris, 28 de junho de 2011. Disponível em: <http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/479&format=HTML&aged=0&language=EN&guiLanguage=en>. Acesso em 20 de julho de 2012.

papel dos princípios seria apontar aquilo que a Internet tem de essencial, que deve ser promovido ou preservado.[88] A Comissão Europeia formulou o esboço de um rol de princípios, que ficou conhecido como *Digital Compact for the Internet* (em inglês, a primeira letra de cada um dos princípios forma a palavra "compact"). A iniciativa foi formalmente apresentada no Fórum de Governança da Internet de 2011, em Nairóbi, e aborda tópicos importantes, como a necessidade de preservar as características fundamentais da arquitetura de rede, de evitar a fragmentação e de fazer uso da Internet para o fortalecimento da democracia. De modo resumido, os princípios seriam os seguintes:

Responsabilidade cívica. Assim como no ambiente *off-line*, as pessoas assumem responsabilidades umas com as outras na Internet, que vão além das puramente legais.

Uma Internet. É preciso evitar a fragmentação.

Governança multissetorial da Internet. A participação de todos os interessados na formulação de políticas é positiva.

Pró-democracia. Com as ferramentas certas, a Internet pode se tornar um instrumento de apoio à vida democrática.

Questões de arquitetura. A arquitetura da Internet é fundamental para a sua dinâmica. A arquitetura vai mudar no futuro, com o surgimento de novos desafios, mas é preciso estar ciente das implicações que diferentes modelos possam ter.

A confiança dos usuários é um pré-requisito. Barreiras para a confiança são barreiras ao acesso. Se não forem solucionados, problemas como a proteção aos dados pessoais, à privacidade e à segurança podem afastar as pessoas da rede.

Governança transparente. Essa seria a base de sustentação do multissetorialismo. Em particular, é preciso transparência sobre o papel do governo ao representar seus cidadãos, e garantir que opiniões não sejam ignoradas.

A comissária Neelie Kroes fez algumas observações sobre o princípio do multissetorialismo e alertou para riscos de captura dos espaços multissetoriais por interesses privados durante a sua intervenção no IGF 2011. "Em última instância, diferentes atores têm diferentes áreas de *expertise* e responsabilidades. As autoridades públicas têm uma responsabilidade especial de lidar com questões de ordem pública, tanto *on-line* como *off-line*, e isso deve ser refletido no processo

[88] KROES, Neelie. Cerimônia de abertura do Fórum de Governança da Internet. Nairobi, 2011. Disponível em: <http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/605&format=HTML&aged=0&language=EN&guiLanguage=en>. Acesso em 20 de julho de 2012.

de tomada de decisão. Caso contrário, o resultado do multissetorialismo será o sequestro da tomada de decisões por lobistas, e o interesse privado se passará por interesse público".[89]

A Comissão Europeia parece ser um dos atores que defendem uma reformulação nos mecanismos de governança da Internet, sobretudo para reforçar a participação governamental: "Não estamos sugerindo uma alternativa ao modelo multissetorial de Governança da Internet, só que ele precisa ser alterado para funcionar melhor e ter em conta a voz dos governos".[90] Levando em consideração os principais comunicados e documentos produzidos pela Comissão, seu posicionamento em relação aos mecanismos de governança parece ter como objetivo principal o intuito de rever e ampliar o espaço de participação dos governos no âmbito da ICANN.[91]

A inciativa da Comissão Europeia, visando delinear princípios fundamentais, é muito bem-vinda diante do complexo mapa político e institucional da União. Todavia, diferentemente de outros países que começaram a aprovar medidas de regulação da Internet nos últimos anos, a União e vários Estados membros possuem uma malha regulatória já robusta sobre o tema, assim como práticas já consolidadas, o que pode trazer dificuldades para a implementação concreta dos princípios.

Poderá ser um grande desafio conciliar, por exemplo, o princípio que versa sobre a preservação da arquitetura, com evidências de que os operadores de telecomunicações restringem o acesso de seus usuários à Internet, violando a neutralidade da rede[92]. Segundo La Quadrature du Net, a liberdade de expressão, a privacidade, a inovação e a concorrência estão sendo prejudicados pelas práticas dos operadores[93]. De igual maneira, pode-se prever conflitos entre princípios que visem a promoção da confiança dos usuários e o receio provocado por um ambiente de permanente vigilância, criado pela aprovação de leis como a Hadopi na França (Tópico 9.3.1.), que prevê a suspensão do acesso à Internet

---

[89] Ibidem.

[90] KROES, Neelie. *European Dialogue on Internet Governance (EuroDIG)*. Belgrado, 2011. Disponível em: <http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/419>. Acesso em 20 de julho de 2012.

[91] MCCARTHY, Kieren. *European Commission Papers on ICANN: what they actually say*. Disponível em: <http://news.dot-nxt.com/2011/08/31/ec-papers-details>. Acesso em 20 de julho de 2012.

[92] *La Quadrature du Net*. Disponível em: <https://www.laquadrature.net/en/Net_neutrality>. Acesso em 20 de julho de 2012.

[93] Disponível em: <https://www.laquadrature.net/en/more-than-half-of-the-eu-with-restrictions-to-net-access-what-will-neelie-kroes-do>. Acesso em 20 de julho de 2012.

de indivíduos que reincidam na prática de *download* de arquivos protegidos por direito autoral.

6.3.4 Estados Unidos e a estratégia internacional para o ciberespaço

Em maio de 2011, o presidente Barack Obama anunciou um plano estratégico para o ciberespaço com princípios que devem guiar o desenvolvimento transversal de políticas relacionadas à Internet no âmbito do governo americano.[94] O enfoque principal da inciativa se encontra na segurança: o documento reconhece o papel que a Internet desempenha no desenvolvimento econômico e social, mas também as novas ameaças que se perpetuam por meio da rede. Dentre elas, figuram "os desastres naturais, sabotagens, o roubo da propriedade intelectual e a possibilidade de ameaças à paz e à segurança internacional".

O documento afirma a intenção do governo de buscar o equilíbrio entre liberdade e segurança em todas as políticas governamentais: "boas políticas de segurança cibernética podem reforçar a privacidade e a aplicação eficaz da lei. Ao mirar comportamentos amplamente reconhecidos como ilegais, podem proteger as liberdades fundamentais". No âmbito internacional, uma das metas do governo americano seria ampliar a adesão dos países à Convenção de Budapeste sobre cibercrimes.

O documento destaca o papel de *softwares* proprietários e abertos para a economia e para a plena satisfação das necessidades dos usuários, e chama atenção para a importância da interoperabilidade e da preservação da arquitetura *end to end*, no intuito de evitar a fragmentação da rede. Afirma-se que "os métodos usados por um país para bloquear *websites* podem trazer uma perturbação em cascata muito maior em rede internacional". No entanto, não há no documento indícios de que o governo dos Estados Unidos pretenda alterar sua própria política de apreensão de *websites*, que vem produzindo efeitos extraterritoriais.[95]

A importância da participação multissetorial na governança da Internet é destacada ao longo do documento. O governo dos Estados Unidos reconhece a

---

[94] *International strategy for cyberspace: prosperity, security and openess in a networked world*. Maio, 2011. Disponível em: <http://www.whitehouse.gov/sites/default/files/rss_viewer/internationalstrategy_cyberspace.pdf>. Acesso em 20 de julho de 2012.

[95] *Ars Technica. Senator: domain name seizures "alarmingly unprecedented"*. Disponível em: <http://arstechnica.com/tech-policy/news/2011/02/senator-us-domain-name-seizures-alarmingly-unprecedented.ars>. Acesso em 20 de julho de 2012.

importância do IGF e de fóruns "que representam toda a comunidade da Internet através da integração do setor privado, sociedade civil, academia, bem como dos governos em um ambiente multissetorial". Mais adiante, o documento dá um destaque especial à relevância das parcerias entre o governo e o setor privado, sugerindo que a participação desses atores nos arranjos de governança teria importância estratégica para o governo dos EUA: "Embora o setor privado já desempenhe um papel importante nas organizações internacionais e multissetoriais, vamos continuar a alavancar mecanismos existentes de parceria para colaborar com parceiros da indústria. Em particular, trabalharemos em estreita colaboração com os proprietários de infraestrutura e operadores (...). Buscamos a participação do setor privado na governança da Internet, que é essencial para a defesa de seu caráter multissetorial, e continuaremos a defender a sua inclusão nas instâncias que se dedicam a tais questões".

O documento elenca, por fim, as políticas que serão prioridade para o governo dos Estados Unidos:

Economia: promoção de normas internacionais e mercados abertos e inovadores

- Manter um ambiente de livre comércio que estimule a inovação tecnológica em redes acessíveis, globalmente interligadas;
- Proteger a propriedade intelectual, incluindo os segredos comerciais, do roubo;
- Assegurar a primazia de padrões técnicos interoperáveis e seguros, determinados por especialistas técnicos.

Proteger nossas redes: reforçar a segurança, a confiabilidade e a resiliência

- Promover a cooperação no ciberespaço, em especial sobre normas de comportamento para os Estados e sobre segurança cibernética, bilateralmente e no âmbito de organizações multilaterais e parcerias multinacionais;
- Reduzir intrusões e interrupções na rede dos Estados Unidos;
- Assegurar um mecanismo robusto de administração de incidentes, a resiliência e a capacidade de recuperação da infraestrutura de informação;
- Melhorar a segurança da cadeia de fornecimento de alta tecnologia.

Impor a lei: estender a colaboração e o Estado de Direito

- Participar plenamente das discussões internacionais sobre cibersegurança;
- Harmonizar as leis internacionais de cibercrime, expandindo a adesão à Convenção de Budapeste;
- Concentrar as leis de cibercrime na luta contra as atividades ilegais, sem restringir o acesso à Internet;
- Negar aos terroristas e a outros criminosos a capacidade de explorar a Internet para operacionalização de planejamento, financiamento, ou ataques.

continuação >

Militar: preparar-se para os desafios de segurança do século 21

- Reconhecer e se adaptar à necessidade militar crescente de redes confiáveis e seguras;
- Construir e reforçar alianças militares existentes para enfrentar potenciais ameaças no ciberespaço;
- Expandir a cooperação com aliados e parceiros para aumentar a segurança coletiva

Governança da Internet: promoção de estruturas eficazes e inclusivas

- Priorizar a abertura e a inovação na Internet;
- Preservar a segurança e a estabilidade mundiais da rede, incluindo o sistema de nome de domínio (DNS);
- Promover e melhorar fóruns multissetoriais para a discussão da governança da Internet.

Desenvolvimento internacional: capacitação, segurança e prosperidade

- Fornecer conhecimento, treinamento e outros recursos para países que buscam desenvolver a capacidade técnica e de segurança cibernética;
- Desenvolver continuamente e compartilhar regularmente melhores práticas de cibersegurança internacionais;
- Aumentar a capacidade dos Estados para combater o cibercrime, incluindo treinamento para aplicação da lei, direcionado a especialistas forenses, juristas e legisladores;
- Desenvolver relações com os formuladores de políticas para melhorar a capacitação técnica, estabelecendo contato permanente com especialistas parceiros em outros países.

Liberdade na Internet: apoio às liberdades fundamentais e à privacidade

- Apoiar os atores da sociedade civil para obter plataformas confiáveis e seguras para o exercício das liberdades de expressão e de associação;
- Colaborar com a sociedade civil e organizações não governamentais para estabelecer salvaguardas que protejam suas atividades na Internet de invasões ilegais;
- Incentivar a cooperação internacional para a efetiva proteção à privacidade de dados no comércio;
- Garantir a interoperabilidade *end to end* em uma Internet acessível a todos.

6.3.5 Discussões sobre princípios no âmbito do G8

Em 2011, o G8 tratou pela primeira vez do tema da governança da Internet no nível de sua reunião de cúpula, que congrega chefes de Estado e de Governo. A declaração final da cúpula do G8 [96] elencou uma série de princípios, discutidos no e-G8, evento realizado antes da cúpula oficial. O e-G8 contou com a partici-

[96] CÚPULA DE DEAUVILLE. Declaração do G8. *Renewed Commitment For Freedom And Democracy.* Maio de 2011. Disponível em: <http://www.g20-g8.com/g8-g20/g8/english/live/news/renewed-commitment-for-freedom-and-democracy.1314.html>. Acesso em 20 de julho de 2012.

pação de representantes das principais empresas ligadas à Internet, porém houve pouca possibilidade de envolvimento da sociedade civil. Isso gerou críticas, tendo-se afirmado que o evento "descarta o princípio da participação multissetorial, que tem evoluído no plano mundial".[97] Além disso, destacou-se que "políticas definidas em conjunto pelas nações mais poderosas muito provavelmente se tornarão a norma padrão global (...). Assim, é conveniente que os países do G8 discutam essas e outras questões em fóruns globais mais democráticos, onde todos os países estejam presentes em pé de igualdade".[98]

Entidades da sociedade civil que participaram do e-G8 apontaram que a mensagem enviada pelo evento foi dúbia. Se, por um lado, mencionaram-se princípios importantes, como a liberdade de expressão, o respeito à privacidade e à participação multissetorial, houve, por outro, ênfase no combate ao cibercrime e à proteção à propriedade intelectual *on-line*, sem deixar claro os meios que seriam utilizados para isso e sem avaliar como eles poderiam impactar o acesso e o livre tráfego dos dados na rede.

A organização Artigo 19 afirmou que a declaração não reconheceu a proteção dos direitos humanos "como um princípio fundamental acima de todos os outros", tendo dado mais ênfase a preocupações de cunho econômico, sobretudo a proteção à propriedade intelectual, na medida em que parece endossar novas restrições à liberdade de expressão na Internet, fortalecendo o *enforcement* da propriedade intelectual e indo ao encontro de propostas polêmicas, como o acordo anticontrafação (ACTA) e de leis nacionais que preveem a resposta graduada ou *three strikes*.[99]

Não houve referência direta à importância do princípio da neutralidade da rede ou ao papel que as grandes empresas, muitas delas baseadas nos países desenvolvidos, desempenham nas políticas de censura ou *enforcement*. Sem a abordagem desses temas, as discussões no G8 parecem pouco propensas a causar um impacto positivo concreto sobre a promoção de direitos e da liberdade de expressão na Internet.

---

[97] INTERNET GOVERNANCE CAUCUS. *Open letter to President Sarkozy on eG20 meeting plan*. Disponível em: <http://www.igcaucus.org/open-letter-president-sarkozy-eg8-meeting-plan>. Acesso em 20 de julho de 2012.

[98] Ibidem.

[99] *Article* 19. "*G8: the Deauville Declaration on Internet Fails to Recognise Importance of Human Rights Including Freedom of Expression*. Disponível em: <http://www.article19.org/data/files/pdfs/press/g8-the-deauville-declaration-on-internet-fails-to-recognise-importance-of-hu.pdf>. Acesso em 20 de julho de 2012.

TABELA 1: COMPARAÇÃO DE PRINCÍPIOS DO CGI.BR, DO MARCO CIVIL DA INTERNET NO BRASIL, DA DECLARAÇÃO DO CONSELHO DA EUROPA (JUNHO DE 2011), DO *COMUNIQUÉ* DA OCDE (JULHO DE 2011), DA ESTRATÉGIA INTERNACIONAL PARA O CIBERESPAÇO DOS EUA (MAIO DE 2011), DA PROPOSTA DA UNIÃO EUROPEIA (JULHO DE 2011) E DA DECLARAÇÃO DO G8 (MAIO DE 2011). ADAPTADO DE WOLFGANG KLEINWACHTER – A FEBRE DOS PRINCÍPIOS DA INTERNET. REVISTA POLITICS N. 10 – AGOSTO DE 2011

Assunto	CGI.br	Marco Civil da Internet no Brasil (PL 2126/2011)	Conselho da Europa	OCDE	EUA	UE	G8
Direitos Humanos	[1] Liberdade, privacidade e direitos humanos	[art. 2º, II] Direitos humanos e cidadania [art. 2º, III] Pluralidade e Diversidade [art. 3º, I e II, art. 7, Parágrafo único, art. 8º, art. 10] Proteção da privacidade e dos dados pessoais [art. 3º, III] Liberdade de expressão, comunicação e manifestação [art. 7°, I] Inviolabilidade e sigilo das comunicações [art. 7°, II] não-suspensão da conexão [art 7°, III] Manutenção da qualidade contratada [art. 7°, IV] Acesso a informações claras e completas constantes dos contratos de prestação de serviços [art. 7°, V] não fornecimento a terceiros de registros de conexão e de acesso a aplicações de Internet [art. 19, VIII] promoção da cultura e da cidadania	[1] Direitos humanos, democracia e leis	[1] Livre fluxo de informação global	[1] Suporte às liberdades fundamentais	[4] Pró-democracia	[1] Liberdade
	[5] Diversidade Cultural		[10] Diversidade linguística e cultural	[9] Proteção à privacidade	[3] Valorização da privacidade		[2] Proteção da privacidade

continuação >

TABELA 1: COMPARAÇÃO DE PRINCÍPIOS DO CGI.BR, DO MARCO CIVIL DA INTERNET NO BRASIL, DA DECLARAÇÃO DO CONSELHO DA EUROPA (JUNHO DE 2011), DO *COMUNIQUÉ* DA OCDE (JULHO DE 2011), DA ESTRATÉGIA INTERNACIONAL PARA O CIBERESPAÇO DOS EUA (MAIO DE 2011), DA PROPOSTA DA UNIÃO EUROPEIA (JULHO DE 2011) E DA DECLARAÇÃO DO G8 (MAIO DE 2011). ADAPTADO DE WOLFGANG KLEINWACHTER – A FEBRE DOS PRINCÍPIOS DA INTERNET. REVISTA POLITICS N. 10 – AGOSTO DE 2011

Assunto	CGI.br	Marco Civil da Internet no Brasil (PL 2126/2011)	Conselho da Europa	OCDE	EUA	UE	G8
Segurança	[7] Inimputabilidade da rede	[art. 3º, VI] Responsabilização dos agentes de acordo com suas atividades [art. 14]. O provedor de conexão à Internet não será responsabilizado por danos decorrentes de conteúdo gerado por terceiros [art. 15] O provedor de aplicações de Internet somente poderá ser responsabilizado por conteúdo gerado por terceiros se, após ordem judicial, não tomar as providências para tornar indisponível o conteúdo apontado como infringente	[3] Responsabilidade dos Estados	[5] Base de dados confiável para a formulação de políticas	[4] Proteção contra crimes	[1] Responsabilidade Cívica	[2] Cibersegurança
			[6] Integridade da Internet	[6] Transparência, processo justo e prestação de contas	[5] Direito de autodefesa		[3] Proteção contra crimes
				[13] Cooperação para a segurança na Internet	Cibersegurança e investigação rigorosa		

continuação >

TABELA 1: COMPARAÇÃO DE PRINCÍPIOS DO CGI.BR, DO MARCO CIVIL DA INTERNET NO BRASIL, DA DECLARAÇÃO DO CONSELHO DA EUROPA (JUNHO DE 2011), DO *COMUNIQUÉ* DA OCDE (JULHO DE 2011), DA ESTRATÉGIA INTERNACIONAL PARA O CIBERESPAÇO DOS EUA (MAIO DE 2011), DA PROPOSTA DA UNIÃO EUROPEIA (JULHO DE 2011) E DA DECLARAÇÃO DO G8 (MAIO DE 2011). ADAPTADO DE WOLFGANG KLEINWACHTER – A FEBRE DOS PRINCÍPIOS DA INTERNET. REVISTA POLITICS N. 10 – AGOSTO DE 2011

Assunto	CGI.br	Marco Civil da Internet no Brasil (PL 2126/2011)	Conselho da Europa	OCDE	EUA	UE	G8
Governança	[2] Governança democrática e colaborativa	[art. 3º, VII] Preservação da natureza participativa da rede [art. 19, I] estabelecimento de mecanismos de governança transparentes, colaborativos e democráticos, com a participação dos vários setores da sociedade	[3] Governança Multissetorial	[5] Processos multissetoriais de desenvolvimento de políticas	[9] Governança multissetorial	[3] Governança multissetorial	[4] Governança multissetorial
			[4] Empoderamento dos usuários	[6] Códigos de comportamento voluntariamente desenvolvidos		[7] Governança transparente	
	[10] Ambiente legal e regulatório – deve preservar a Internet como espaço de colaboração		[7] Gerência descentralizada	[10] Empoderamento e responsabilidade do indivíduo			
				[14] Aplicação e execução das normas			

continuação >

TABELA 1: COMPARAÇÃO DE PRINCÍPIOS DO CGI.BR, DO MARCO CIVIL DA INTERNET NO BRASIL, DA DECLARAÇÃO DO CONSELHO DA EUROPA (JUNHO DE 2011), DO *COMUNIQUÉ* DA OCDE (JULHO DE 2011), DA ESTRATÉGIA INTERNACIONAL PARA O CIBERESPAÇO DOS EUA (MAIO DE 2011), DA PROPOSTA DA UNIÃO EUROPEIA (JULHO DE 2011) E DA DECLARAÇÃO DO G8 (MAIO DE 2011). ADAPTADO DE WOLFGANG KLEINWACHTER – A FEBRE DOS PRINCÍPIOS DA INTERNET. REVISTA POLITICS N. 10 – AGOSTO DE 2011

Assunto	CGI.br	Marco Civil da Internet no Brasil (PL 2126/2011)	Conselho da Europa	OCDE	EUA	UE	G8
Tecnologia/ arquitetura	[3] Universalidade	[art. 2º, IV] Abertura e Colaboração [art. 3º, IV] Neutralidade da rede [art. 3º, V] Estabilidade, segurança e funcionalidade [art. 9º] O responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicativo, sendo vedada qualquer discriminação ou degradação do tráfego que não decorra de requisitos técnicos necessários à prestação adequada dos serviços, conforme regulamentação	[5] Universalidade da Internet	[2] Internet aberta, distribuída e interconectada	[6] Interoperabilidade Global	[2] Uma Internet	
	[6] Neutralidade da rede		[8] arquitetura aberta		[7] Estabilidade da rede	[5] Arquitetura aberta	
	[8] Funcionalidade, segurança e estabilidade		[9] rede aberta		[8] Acesso confiável		
	[9] Padronização e interoperabilidade						

continuação >

TABELA 1: COMPARAÇÃO DE PRINCÍPIOS DO CGI.BR, DO MARCO CIVIL DA INTERNET NO BRASIL, DA DECLARAÇÃO DO CONSELHO DA EUROPA (JUNHO DE 2011), DO *COMUNIQUÉ* DA OCDE (JULHO DE 2011), DA ESTRATÉGIA INTERNACIONAL PARA O CIBERESPAÇO DOS EUA (MAIO DE 2011), DA PROPOSTA DA UNIÃO EUROPEIA (JULHO DE 2011) E DA DECLARAÇÃO DO G8 (MAIO DE 2011). ADAPTADO DE WOLFGANG KLEINWACHTER – A FEBRE DOS PRINCÍPIOS DA INTERNET. REVISTA POLITICS N. 10 – AGOSTO DE 2011

Assunto	CGI.br	Marco Civil da Internet no Brasil (PL 2126/2011)	Conselho da Europa	OCDE	EUA	UE	G8
Economia	[5] Inovação	[art. 2º, V] a livre iniciativa, a livre concorrência e a defesa do consumidor [art. 19, VI] otimização da infraestrutura das redes, promovendo a qualidade técnica, a inovação e a disseminação das aplicações de Internet, sem prejuízo à abertura, à neutralidade e à natureza participativa;		[3] Investimento e competitividade em banda larga e alta velocidade [15] Entrega de serviços transfronteiras [11] Criatividade e inovação [12] Limites para as responsabilidades e obrigações de intermediários	[2] Respeito à propriedade	[6] Confiança para o usuário	[3] Proteção à propriedade Intelectual

continuação >

TABELA 1: COMPARAÇÃO DE PRINCÍPIOS DO CGI.BR, DO MARCO CIVIL DA INTERNET NO BRASIL, DA DECLARAÇÃO DO CONSELHO DA EUROPA (JUNHO DE 2011), DO *COMUNIQUÉ* DA OCDE (JULHO DE 2011), DA ESTRATÉGIA INTERNACIONAL PARA O CIBERESPAÇO DOS EUA (MAIO DE 2011), DA PROPOSTA DA UNIÃO EUROPEIA (JULHO DE 2011) E DA DECLARAÇÃO DO G8 (MAIO DE 2011). ADAPTADO DE WOLFGANG KLEINWACHTER – A FEBRE DOS PRINCÍPIOS DA INTERNET. REVISTA POLITICS N. 10 – AGOSTO DE 2011

Assunto	CGI.br	Marco Civil da Internet no Brasil (PL 2126/2011)	Conselho da Europa	OCDE	EUA	UE	G8
Os princípios abaixo encontram-se presentes no Marco Civil da Internet no Brasil, mas não faziam parte dos parâmetros iniciais de comparação entre as propostas de princípios, razão pela qual aparecem separados dos demais.							
Governo eletrônico/ Governo Aberto		[art. 19, II, III] interoperabilidade tecnológica dos serviços de governo eletrônico, entre os diferentes Poderes e níveis da federação. Interoperabilidade entre sistemas e terminais diversos, inclusive entre os diversos setores da sociedade [art. 19, IX; art. 20, IV] prestação de serviços públicos de atendimento ao cidadão de forma integrada, eficiente, simplificada e por múltiplos canais de acesso [art. 20, I] compatibilidade dos serviços de governo eletrônico com diversos terminais, sistemas operacionais e aplicativos [art. 20, III] compatibilidade tanto com a leitura humana quanto com o tratamento automatizado das informações [art. 20, V] fortalecimento da participação social nas políticas públicas						

continuação >

TABELA 1: COMPARAÇÃO DE PRINCÍPIOS DO CGI.BR, DO MARCO CIVIL DA INTERNET NO BRASIL, DA DECLARAÇÃO DO CONSELHO DA EUROPA (JUNHO DE 2011), DO *COMUNIQUÉ* DA OCDE (JULHO DE 2011), DA ESTRATÉGIA INTERNACIONAL PARA O CIBERESPAÇO DOS EUA (MAIO DE 2011), DA PROPOSTA DA UNIÃO EUROPEIA (JULHO DE 2011) E DA DECLARAÇÃO DO G8 (MAIO DE 2011). ADAPTADO DE WOLFGANG KLEINWACHTER – A FEBRE DOS PRINCÍPIOS DA INTERNET. REVISTA POLITICS N. 10 – AGOSTO DE 2011

Assunto	CGI.br	Marco Civil da Internet no Brasil (PL 2126/2011)	Conselho da Europa	OCDE	EUA	UE	G8
Acessibilidade		[art. 20, II] acessibilidade a todos os interessados, independentemente de suas capacidades físico-motoras, perceptivas, culturais e sociais					
Desenvolvimento de Capacidades		[art. 19, VII] desenvolvimento de ações e programas de capacitação para uso da Internet [art. 21] O cumprimento do dever constitucional do Estado na prestação da educação, em todos os níveis de ensino, inclui a capacitação para o uso seguro, consciente e responsável da Internet como ferramenta para o exercício da cidadania, a promoção de cultura e o desenvolvimento tecnológico					

6.4 Aperfeiçoamento do Fórum de Governança da Internet (IGF)

O IGF é um dos principais resultados das discussões da Cúpula Mundial da Sociedade da Informação (CMSI), ocorrida em duas fases, em 2003 e 2005.[100] Seus participantes pediram ao Secretário Geral da ONU que criasse, em um processo aberto e inclusivo, um novo fórum para o debate multissetorial de políticas relacionadas à rede.[101] O IGF é hoje o principal fórum em que ocorre a discussão, de modo transversal, de uma ampla gama de temas, como acesso, privacidade, abertura e segurança.

A característica multissetorial do IGF significa que governos, sociedade civil, academia, comunidade técnica e setor empresarial participam de forma conjunta e em igualdade de condições nas discussões no Fórum. Diante disso, o IGF cria oportunidades para sinergia, para a identificação de temas emergentes e para a consolidação de parcerias.

O IGF realizou-se na Grécia (2006), no Brasil (2007), na Índia (2008), no Egito (2009), na Lituânia (2010) e no Quênia (2011). Após cinco anos, encerrou-se o mandato inicial do Fórum, que foi renovado até 2015. Segundo a resolução[102] da Assembleia Geral da ONU, o Fórum deveria ser aperfeiçoado com o objetivo de conectá-lo ao diálogo sobre governança da Internet no plano global.

O processo de discussão sobre aperfeiçoamento do IGF ficou sob responsabilidade da Comissão de Ciência e Tecnologia para o Desenvolvimento (CSTD) da ONU, no âmbito da qual foi criado um Grupo de Trabalho que deveria buscar, compilar e analisar contribuições de todos os Estados membros e todas as outras partes interessadas e fazer recomendações.[103]

As discussões no Grupo de Trabalho foram agrupadas em eixos: 1) resultados das discussões no IGF; 2) modalidades de trabalho, incluindo as consultas abertas, o funcionamento do secretariado e o papel do Grupo Consultivo Multissetorial (*Multistakeholder Advisory Group* – MAG); 3) financiamento do IGF; 4) ampliação

---

[100] *World Summit on the Information Society*. Disponível em: <http://www.itu.int/wsis/index.html>. Acesso em 20 de julho de 2012.

[101] Agenda de Túnis (parágrafo 72), endossada. Resolução 60/252 da Assembleia Geral da ONU.

[102] Disponível em: <http://unpan1.un.org/intradoc/groups/public/documents/un-dpadm/unpan039074.pdf>. Acesso em 15 de agosto de 2012.

[103] Grupo de Trabalho sobre aperfeiçoamentos ao IGF. Disponível em: <http://www.unctad.info/en/CstdWG/>. Acesso em 20 de julho de 2012.

da participação; 5) conexão entre o IGF e outros processos, mecanismos e órgãos que tratam de temas relacionados à governança da Internet.

O Grupo de Trabalho reuniu-se durante o ano de 2011 e deve concluir seu relatório em 2012, encaminhando-o para o Conselho Econômico e Social das Nações Unidas (ECOSOC). Durante as discussões, consensos importantes foram atingidos, como um entendimento geral sobre o fato de que o IGF deve produzir resultados mais concretos – que captem as convergências e as diferentes visões sobre questões específicas de política pública –, que possam ser compartilhados com atores e organizações relevantes no regime de governança da Internet.

Concordou-se que deve haver medidas voltadas à ampliação da participação presencial no Fórum, sobretudo de atores de países em desenvolvimento e de países menos avançados. A participação remota foi apontada como parte integrante da dinâmica do IGF, e reconheceu-se a necessidade de dotá-la de recursos necessários ao seu pleno funcionamento. Por outro lado, o modelo de financiamento do fórum, baseado apenas em doações voluntárias, permanecerá o mesmo, o que poderia limitar a implementação das sugestões de aperfeiçoamento.

6.5 Pressões pela implementação do mecanismo de cooperação aprimorada, presente na Agenda de Túnis da Cúpula Mundial da Sociedade da Informação

A cooperação aprimorada foi um dos resultados das discussões na Cúpula Mundial da Sociedade da Informação (CMSI). De acordo com o parágrafo 69 da Agenda de Túnis, seria um mecanismo para "permitir que os governos, em pé de igualdade, desempenhassem suas funções e responsabilidades em questões de política pública relacionadas com a Internet, mas não no dia a dia das questões técnicas e operacionais, que não tem impacto sobre questões de política pública".

A definição vaga de cooperação aprimorada, presente na Agenda de Túnis, tem gerado divergências sobre a implementação do mecanismo. Alguns atores acreditam que ele deve se traduzir em uma coordenação mais formal e estreita entre as organizações que lidam com temas relacionados à governança. Outros atores pleiteiam que os temas sejam discutidos em um fórum multilateral, existente ou a ser criado, no âmbito da ONU. Argumentam que a tomada de decisões sobre as políticas públicas relacionadas à Internet está ocorrendo atualmente em fó-

runs de participação limitada, como a OCDE ou o Conselho da Europa, nos quais os países em desenvolvimento não se fazem presentes.

A discussão sobre cooperação aprimorada intensificou-se desde 2010, quando uma série de consultas e reuniões foi realizada pelo Departamento de Assuntos Econômicos e Sociais da ONU (DESA). Recentemente, uma série de reuniões para tentar conciliar os posicionamentos acerca do tema foi marcada para 2012, no âmbito da Comissão de Ciência e Tecnologia da ONU, em Genebra. Entrementes, países de diversas matizes políticas e ideológicas têm buscado marcar posição e delinear, ainda que de modo geral, a sua compreensão sobre o papel do Estado e dos órgãos multilaterais na governança da Internet. Vários documentos produzidos recentemente possuem relação explícita ou implícita com a discussão sobre cooperação aprimorada e devem ser entendidos no âmbito desse contexto político.

6.6 Código de conduta internacional sobre segurança da informação proposto por China, Rússia, Tadjiquistão e Uzbequistão

A proposta de resolução (A/66/359)[104] foi submetida aos países membros da ONU na 66ª reunião da Assembleia Geral. O código de conduta deveria servir como parâmetro para as regras, visando prevenir o uso das tecnologias da informação e comunicação para fins que sejam incompatíveis com os objetivos da manutenção da estabilidade e da segurança internacionais, que podem afetar adversamente a integridade da infraestrutura nos Estados, em detrimento da sua segurança. Segundo a proposta, o código de conduta seria aberto à adesão voluntária dos Estados que desejassem ingressar em seu domínio jurídico.

Se, por um lado, a proposta de código afirma que os países devem respeitar "direitos humanos e liberdades fundamentais", por outro, o documento visa "coibir a divulgação de informações que incitem o terrorismo, a secessão e o extremismo, ou que comprometam a estabilidade política, econômica e social de outros países, bem como seu ambiente espiritual e cultural". A generalidade do texto deixa ampla margem para a repressão do legítimo exercício da liberdade de

[104] *International Code of Conduct for Information Security*. Disponível em: <http://nz.chineseembassy.org/eng/zgyw/t858978.htm>. Acesso em 20 de julho de 2012.

expressão e pode constranger os signatários a observar parâmetros legislativos mais restritivos do que aqueles atualmente em vigor.

6.7 I Fórum IBAS sobre governança da Internet

O IBAS é um mecanismo de diálogo permanente criado em 2003 entre Índia, Brasil e África do Sul. Seus principais objetivos são promover a concertação política, buscar a democratização dos fóruns internacionais, ampliando a participação dos países em desenvolvimento, promover a cooperação cultural, técnica e científica e implementar medidas de promoção do desenvolvimento.

O Fórum IBAS sobre Governança da Internet foi realizado em setembro de 2011 na Fundação Getulio Vargas do Rio de Janeiro. O evento foi patrocinado pelo Ministério das Relações Exteriores e contou com o apoio do Comitê Gestor da Internet (CGI.br) e do Centro de Tecnologia e Sociedade (CTS/FGV). O objetivo do encontro foi discutir questões substantivas e institucionais que estão na agenda da governança da Internet, buscando identificar os interesses e prioridades dos atores dos três países.

A partir de um mapa geral de reflexões socioeconômicas sobre o desenvolvimento e o acesso à Internet, houve a discussão de temas específicos, como infraestrutura, recursos críticos, princípios regulatórios e arranjos institucionais. Outras questões foram destacadas como importantes e requerem aprofundamento, como o tema da competência jurisdicional, do comércio eletrônico e das questões fiscais, dos padrões abertos, da neutralidade da rede e da convergência de mídias.

No que diz respeito às discussões sobre arranjos institucionais, os participantes reconheceram o papel importante que o IGF desempenha no regime de Governança da Internet, como um espaço de sensibilização, de capacitação e de identificação de questões de políticas públicas. Ao mesmo tempo, alguns dos participantes argumentaram que os atuais mecanismos não implementam o ideal de uma cooperação aprimorada, prevista na Agenda de Túnis.

A organização indiana *IT for Change* apresentou um documento como contribuição às discussões do Fórum, em que aponta alguns dos temas mais relevantes para os países em desenvolvimento:[105]

---

[105] *IT for Change. A Development Agenda in Internet Governance: Outlining Global Public Policy Issues and Exploring New Institutional Options.* Contribuição preliminar ao seminário do IBAS sobre governança global da Internet.

Questões transfronteiriças e de jurisdição

Os países em desenvolvimento precisam considerar que os mais importantes "nós" do fluxo de tráfego na Internet se encontram em países do Norte, gerando um poder assimétrico sobre a aplicabilidade de leis na rede. Por exemplo, no início de 2011, o governo dos EUA apreendeu o nome de domínio do Rojadirecta.org, *site* espanhol que fornecia *links* para *streaming* de alguns eventos esportivos. O *site* estava baseado na Espanha e era voltado à população local. Seu modelo foi questionado perante os tribunais espanhóis, que decidiram que o *site* não violava as leis nacionais. Mas os EUA conseguiram apreender o nome de domínio e fechar o *site*, simplesmente porque o nome de domínio .org é gerido por uma entidade registrada nos EUA. Em matéria de arquitetura, os EUA têm controle comparativamente mais amplo sobre a Internet global, e as suas agências executivas e judiciais alavancam cada vez mais este controle.

Propriedade intelectual e acesso ao conhecimento

Uma das características mais importantes da Internet é que ela oferece uma plataforma integrada para a partilha global de informação e conhecimento. Ao mesmo tempo, o conhecimento tornou-se um recurso-chave economicamente, o que torna a sua apropriação uma questão central à agenda econômica dos países desenvolvidos. A Internet está sendo usada como um instrumento de aplicação transfronteiriça de normas de propriedade intelectual de modo extralegal, muitas vezes com o uso de tecnologias invasivas, medidas tecnológicas de proteção (DRMs), ou a utilização dos provedores como uma espécie de "polícia privada" para execução de leis de propriedade intelectual.

Comércio e questões fiscais

Existem dois tipos de questões comerciais implicadas: no primeiro, o uso da Internet se dá apenas para fazer o contato e o pagamento, sendo as mercadorias entregues fisicamente; no segundo, há serviços digitais inteiramente comercializados pela Internet, incluindo a entrega, e muitas vezes o consumo. O segundo tipo cria significativos desafios para a governança. Inúmeros problemas têm surgido em relação à aplicação dos direitos do consumidor nas vendas realizadas remotamente. Além disso, a cobrança de impostos legítimos sobre essas operações é uma questão importante. Enquanto as empresas exportadoras de serviços digitais pagam impostos na jurisdição da sua localização e registro, as autoridades do país onde o consumo de serviços ocorre têm dificuldade para cobrar impostos sobre tais transações. Países desenvolvidos, como os membros da União Europeia, têm feito um trabalho considerável para racionalizar os impostos aplicáveis ao comércio transfronteiriço digital. No entanto, os países em desenvolvimento permanecem à margem desses acordos. A situação torna-se ainda mais complexa quando os serviços são negociados com moedas digitais, como os créditos do Facebook.

Regimes de interconexão

A negociação de acordos de conexão entre a rede nacional e a global é uma questão importante e complexa, ainda à mercê de mercados não regulamentados. A questão das tarifas de interconexão foi apontada pela Agenda de Túnis da Cúpula Mundial sobre a Sociedade da Informação (CMSI) como fundamental para o desenvolvimento, mas pouco foi feito até agora com relação a esse tema.

continuação >

Questões de concorrência na indústria digital global

A indústria global da Internet caracteriza-se por monopólios, devido às economias de escala crescentes, peculiares a esta área. Microsoft, Google, Facebook, Twitter e o iTunes da Apple são excelentes exemplos. Não existem iniciativas para fazer frente a esses comportamentos anticoncorrenciais por meio de regulação adequada: a indústria global da Internet é quase completamente desregulamentada. Duas importantes razões para tal situação são (1) empresas globais da Internet são demasiadamente poderosas para qualquer país em particular, especialmente países em desenvolvimento, para que haja efetiva regulação e (2) quase todas essas empresas são baseadas no Norte, principalmente nos EUA, e são uma peça central da estratégia de controle baseada na propriedade intelectual. A falta de aplicação do direito da concorrência significa que indústrias nascentes dos países em desenvolvimento dificilmente têm chance de se estabelecer no plano global ou em seus próprios países, diante de empresas globais monopolistas ou oligopolistas. Deve-se assegurar não só a abertura da arquitetura técnica da Internet; a arquitetura da indústria da Internet tem que ser mantida suficientemente aberta.

Governança das corporações globais

Plataformas como o Facebook e o Twitter têm sido utilizadas para o ativismo político. Nesse contexto, sua neutralidade e seu compromisso com o princípio da liberdade de expressão se tornam muito importantes. Plataformas e redes sociais têm adotado, aleatória e arbitrariamente, abordagens diversas em diferentes contextos e países. Além disso, o conteúdo pessoal depositado na rede é, cada vez mais, uma parte importante da vida social. É preciso que remédios contra atos arbitrários de empresas estejam facilmente ao alcance dos indivíduos, ainda que elas estejam baseadas em outros países.

Abertura, neutralidade da rede e padrões abertos

A Internet é uma plataforma de comunicação capaz de trazer mudança e inovação, em grande medida por causa de sua arquitetura aberta. No entanto, essa situação começa a se alterar. Os protocolos básicos da Internet ainda estão abertos, mas a Internet é hoje dominada por aplicativos proprietários. Uma grande parte do tráfego da Internet passa por um punhado de megaespaços digitais proprietários. Como a arquitetura da Internet móvel foi construída mais tarde, em um ambiente altamente comercial, aplica-se a ela um regime muito mais fechado e verticalmente integrado. O princípio da neutralidade da rede está sendo erodido rapidamente, sobretudo na Internet móvel.

Segurança

As ameaças à segurança na Internet requerem uma cooperação urgente e sustentada no âmbito global e é preciso encontrar os meios formais adequados para isso. A segurança da infraestrutura pode ser fatalmente atingida a distância, por meio da Internet: em 2011 houve notícias de que um vírus destinado a uma instalação nuclear iraniana foi implantado remotamente. Analistas acreditam que, se o ataque tivesse tido sucesso, poderia não só ter prejudicado gravemente a usina, mas também poderia ter desencadeado um desastre nuclear. Notícias de ciberataques contra sistemas de governo e espionagem industrial na rede são corriqueiras.

continuação >

Mídia

A mídia nacional é uma instituição importante para a governança e para a democracia; ela surgiu como uma grande plataforma de mediação política entre os governos e os cidadãos, mas está mudando rapidamente com o advento da Internet, da IPTV e da convergência. É possível que as leis antigas não possam ser adequadamente aplicadas ao contexto da Internet e que novos quadros regulatórios sejam necessários. Esse é um dos temas que carece de discussão global. Como insculpir e manter eficazes espaços nacionais de mídia no âmbito da Internet global? Quais são as implicações estruturais na esfera pública nacional, nas instituições democráticas e na representação das vozes dos marginalizados? Quem são os interessados nas questões globais de governança da Internet? Essas são algumas das questões-chave no contexto emergente.

Diversidade cultural

A Internet pode ser um ambiente com custo muito reduzido de produção e transmissão de conteúdo e pode representar uma grande oportunidade para promover a diversidade cultural. Isso evidencia a necessidade de políticas eficientes e de apoio às boas práticas.

Desenvolvimento e direitos humanos

A governança da Internet tem profundas implicações para as questões transversais de desenvolvimento e direitos humanos. Para os países em desenvolvimento, a importância da Internet para o desenvolvimento econômico, social e humano é o aspecto determinante de suas perspectivas sobre governança da Internet; no entanto, o desenvolvimento ainda não é visto como uma questão fundamental no âmbito da governança. A Internet também impacta significativamente os direitos humanos em sua vertente positiva e negativa. Grande parte do debate sobre esses direitos na Internet é interpretada quase que exclusivamente sob o aspecto negativo, da não intervenção na esfera individual ou nos direitos civis e políticos. É importante perceber a conexão entre Internet e direitos humanos de uma forma mais holística, levando em consideração seu caráter indivisível. É preciso respeitar os direitos econômicos, sociais e culturais, juntamente com os direitos civis e políticos.

No final do seminário IBAS, em uma reunião intergovernamental, os representantes dos governos elaboraram um documento[106] que deveria servir como contribuição inicial sobre a discussão acerca da cooperação aprimorada. Esse documento foi intensamente discutido durante o IGF 2011, em Nairóbi, no

[106] Disponível em: <http://www.culturalivre.org.br/artigos/IBSA_recommendations_Internet_Governance.pdf>. Acesso em 20 de julho de 2012.

qual os representantes dos governos do IBAS participaram de várias sessões e *workshops*. O governo brasileiro afirmou que o documento formulado no seminário estava aberto a sugestões e modificações e que uma proposta sobre cooperação aprimorada seria elaborada somente após uma discussão com todos os setores interessados.

Na quinta cúpula do IBAS, em outubro de 2011, os líderes dos três países reforçaram o compromisso de buscar posições conjuntas nos temas relacionados à governança da Internet, destacaram a importância de implementar um mecanismo de cooperação aprimorada, tomaram nota das discussões que aconteceram no seminário sobre governança da Internet no Rio de Janeiro e recomendaram o estabelecimento de um observatório que iria monitorar os acontecimentos no campo da governança da Internet, ajudando na disseminação de informações e análises entre os países membros.[107]

Os líderes também abordaram o tema da proteção à propriedade intelectual, enfatizando a "necessidade de um sistema internacional equilibrado de propriedade intelectual que contextualize Direitos de Propriedade Intelectual na estrutura maior do desenvolvimento socioeconômico e encare-os não como fins em si mesmos, mas como um meio de promover inovação, crescimento e desenvolvimento em todos os países". Fizeram também advertências "contra tentativas de desenvolver novas regras internacionais sobre o cumprimento de direitos de propriedade intelectual fora dos fóruns multilaterais, que possam dar livre curso a abusos sistemáticos na proteção de direitos, à construção de barreiras contra o livre comércio e ao enfraquecimento de direitos civis fundamentais"[108].

[107] V CÚPULA DO FÓRUM DE DIÁLOGO ÍNDIA, BRASIL E ÁFRICA DO SUL (IBAS). *Declaração de Tshwane*. 2011. Disponível em: <http://www.itamaraty.gov.br/sala-de-imprensa/notas-a-imprensa/v-cupula-do-forum-de-dialogo-india-brasil-e-africa-do-sul-ibas-2013-18-de-outubro-de-2011-declaracao-de-tshwane>. Acesso em 20 de julho de 2012.

[108] Ibidem.

6.8 Proposta indiana de criação de um Comitê na ONU para políticas relacionadas à Internet

Na 66ª reunião da Assembleia Geral da ONU, a Índia apresentou uma proposta de criação de um Comitê para políticas públicas relacionadas à Internet. De acordo com a proposta indiana, o Comitê teria as seguintes atribuições:

1. Desenvolver e estabelecer políticas públicas internacionais com vista a assegurar a coordenação e a coerência nas questões transversais relacionadas à Internet global;
2. Coordenar e supervisionar os órgãos responsáveis pelo funcionamento técnico e operacional da Internet, incluindo o estabelecimento de padrões globais;
3. Facilitar a negociação de tratados, convenções e acordos na Internet relacionados com políticas públicas;
4. Abordar as questões de desenvolvimento relacionadas à Internet;
5. Promover a proteção dos direitos humanos, ou seja, direitos civis, políticos, sociais, econômicos e culturais, incluindo o direito ao desenvolvimento;
6. Realizar arbitragem e resolução de litígios, sempre que necessário; e
7. Promover a gestão de crises em relação à Internet.

O Comitê seria composto por 50 Estados e contaria com cinco comitês consultivos, responsáveis por aconselhar e assessorar os governos. Ele se reportaria diretamente à Assembleia Geral da ONU e faria recomendações não vinculantes para a consideração, adoção ou implementação pelos órgãos intergovernamentais e organizações internacionais pertinentes. O comitê é apresentado como uma adição e não como um substituto ao IGF. O mecanismo seria financiado através de uma combinação de fundos da ONU e recursos provenientes das taxas de registro de nomes de domínio.

Antecipando críticas à iniciativa, o governo indiano afirma que "a intenção da proposta de um mecanismo multilateral e multissetorial não é 'controlar a Internet' ou permitir que os governos tenham a última palavra na regulação da rede, mas se certificar de que a Internet não será governada unilateralmente, mas sim de forma aberta, democrática, inclusiva e participativa, com o envolvimento de todos os setores interessados".[109]

---

[109] MUELLER, Milton. *A United Nations Committee for Internet-relates policies? A fair assessment*. Disponível em: <http://www.internetgovernance.org/2011/10/29/a-united-nations-committee-for-internet-related-policies-a-fair-assessment/>. Acesso em 20 de julho de 2012.

De fato, o documento recebeu críticas, principalmente acerca dos seguintes pontos:

- O documento poderia provocar uma inversão do atual modelo multissetorial, colocando os atores não governamentais em segundo plano;
- Uma duplicação de fóruns poderia esvaziar o IGF a longo prazo;
- O mecanismo de financiamento não deixa claro se uma taxa adicional seria cobrada sobre os registros de nomes de domínio ou se algum tipo de contribuição seria imposta à ICANN;
- O significado preciso da competência para "coordenar e supervisionar os órgãos responsáveis pelo funcionamento técnico e operacional da Internet" não fica claro no documento. Como identificado em algumas análises, essa competência não aparece no resumo da proposta do Comitê, o que leva a questionar se houve uma real intenção de incluí-la.

Alguns afirmam que é possível que iniciativas como essa levem à emergência de um regime de governança da Internet bifurcado: um eixo seria liderado por instituições organicamente desenvolvidas, com competência técnica, e seria multissetorial; o outro seria liderado pelos governos, tratando de temas de políticas públicas. "Pode ser que estejamos diante não de uma luta mortal entre escolhas polarizadas entre dois regimes de governança distintos, mas sim de uma separação de caminhos entre os governos e as instituições organicamente desenvolvidas, que resolvem sair do caminho um do outro.[110]

Há também análises que defendem a pertinência da proposta apresentada pela Índia, principalmente porque percebem um crescente risco de captura do atual regime de governança por interesses privados de grandes empresas. Segundo essa posição, "seria ingênuo imaginar que a Internet é atualmente regida por redes multissetoriais, que são abertas a todos os interessados, e que a escolha se dá entre, de um lado, a manutenção deste regime descentralizado ou, de outro, a entrega do controle para os governos. Na verdade, algumas das áreas mais importantes de políticas públicas digitais não são regidas por redes multissetoriais, nem por organizações intergovernamentais existentes, mas por governos nacionais e grandes empresas (…). A proposta da Índia pode, pelo menos, democratizar estas decisões em algum grau, se um Comitê da ONU para políticas relacionadas à Internet, adequadamente ligado à esfera pública multissetorial,

[110] Ibidem.

for capaz de estabelecer normas globais para a Internet de forma suficientemente aberta e inclusiva.[111]

É provável que a proposta da Índia volte a ser discutida em 2012, quando uma reunião sobre cooperação aprimorada acontecerá no âmbito da Comissão de Ciência e Tecnologia para o Desenvolvimento da ONU (CSTD).

[111] IGF WATCH. *India's proposal for a UN Committee for Internet-Related Policies (CIRP)*. Disponível em: <http://igfwatch.org/discussion-board/indias-proposal-for-a-un-committee-for-internet-related-policies-cirp>. Acesso em 20 de julho de 2012.

7

Comércio eletrônico

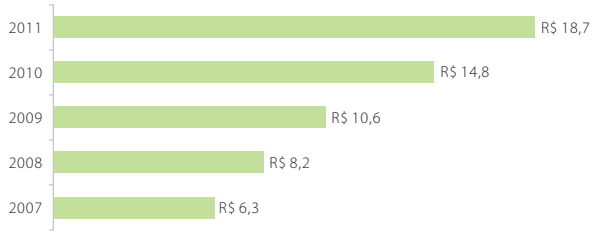
7.1 Comércio eletrônico e atualização do Código de Defesa do Consumidor (CDC)

O comércio eletrônico (também conhecido como *e-commerce*) é toda transação comercial realizada por meio da rede. Desde a criação da Internet, seu uso tem se expandido para se tornar um recurso essencial à vida cotidiana – em outubro de 2011, atingiu mais de 32,2 milhões de usuários únicos, também chamados de e-consumidores[112]. Segundo dados da 25ª edição da pesquisa *Webshoppers*, promovida pela empresa especializada em comércio eletrônico e-bit[113], o faturamento do comércio eletrônico aumentou de 14,8 bilhões de reais em 2010 para 18,7 bilhões de reais em 2011, um aumento de 26% em relação ao ano anterior. A evolução do faturamento do setor entre 2007 e 2011 é ilustrada no gráfico a seguir:

[112] Dados retirados de notícia do *Jornal do Brasil*, disponível em: <http://www.jb.com.br/ciencia-e-tecnologia/noticias/2011/11/28/comercio-eletronico-atingiu-mais-de-32-milhoes-de-usuarios-em-outubro/>. Acesso em 2 de março de 2012.

[113] Dados disponíveis em: <http://www.webshoppers.com.br/webshoppers/WebShoppers25.pdf>. Acesso em 19 de julho de 2012.

EVOLUÇÃO DO FATURAMENTO – E-COMMERCE (EM BILHÕES/R$)



FONTE: E-BIT INFORMAÇÃO (www.ebitempresa.com.br)

Contudo, tem sido frequente a divulgação pela mídia de problemas envolvendo compras no âmbito digital. Esses problemas foram refletidos no *ranking* geral de reclamações do Procon relativo ao ano de 2011[114], no qual o Grupo BW2, detentor das empresas de *e-commerce* Americanas.com, Submarino e Shoptime, ocupa o 2º lugar das empresas que sofreram maior número de reclamações. Essas empresas reuniram um total de 1.574 reclamações, dentre as quais 620 restaram inatendidas. Observa-se uma piora substancial em relação ao ano anterior, em que o grupo ocupou o 21º lugar no *ranking*. A pesquisa afirma, contudo, que essa piora "é reflexo do crescimento do setor de *e-commerce*, meio através do qual muitos dos produtos que são objeto das reclamações no ano passado foram ofertados e adquiridos" (pág. 24).

Considerando esse contexto, o comércio eletrônico foi elencado como um dos temas-chave a serem avaliados pela Comissão de Juristas constituída especialmente para atualizar o Código de Defesa do Consumidor (CDC) – Lei 8.078 de 1990. Essa atualização se faz necessária, portanto, para adequar as normas consumistas à nova realidade de consumo promovida pela Internet, refletida no forte crescimento do *e-commerce* nos últimos anos.

Em paralelo, órgãos de proteção ao consumidor tiveram atuação importante em 2011 em resposta ao crescimento das reclamações envolvendo compras em âmbito digital. O Procon de São Paulo, por exemplo, iniciou a investigação de 20 *sites* que oferecem o serviço de comércio eletrônico[115], devido ao grande número de reclamações de compras efetuadas cujo produto não foi entregue. Durante as

[114] Disponível em: <http://www.procon.sp.gov.br/pdf/acs_ranking_2011.pdf>. Acesso em 17 de julho de 2012.

[115] Retirado da notícia: <http://economia.ig.com.br/financas/seunegocio/procon+sp+denuncia+fraudes+em+sites+de+comercio+eletronico/n1300142822745.html>. Acesso em 7 de março de 2012.

investigações, constatou-se que muitos dos fornecedores, registrados inclusive como pessoa física, não podiam ser encontrados em seus endereços oficiais. Por sua vez, o Núcleo de Defesa do Consumidor (Nudecon), da Defensoria Pública do Estado do Rio de Janeiro, notificou *sites* de venda *on-line* e de compras coletivas para responderem reclamações de consumidores. Entre agosto e dezembro daquele ano, houve aumento de 60% no número de atendimentos pelo Nudecon referentes a compras *on-line*.[116]

A questão também chegou aos tribunais. Segundo dados do Senado Federal, em 2011 foi verificada uma alta taxa de litígios envolvendo relações de consumo, que correspondem a cerca de 20% a 30% dos recursos de julgamentos referentes a direito privado no Superior Tribunal de Justiça. O advento de novas formas de relações de consumo não existentes na época da promulgação do CDC, como as relações comerciais no ambiente digital e, consequentemente, as relações de consumo decorrentes delas, pode ser considerado um dos motivos para esse aumento, uma vez que ainda não são especificamente regulamentadas pelo ordenamento jurídico brasileiro.

Dessa forma, empresas de *e-commerce* e fornecedores que utilizam a Internet em suas transações comerciais acabam por desrespeitar, em muitos casos, as regras gerais de direito do consumidor. Existe, no Brasil, uma dificuldade em precisar as regras relativas à quantidade de informações dispostas no *site* de *e-commerce* sobre o produto e sobre o prazo de entrega do produto ou de devolução do dinheiro em caso de problemas com a compra, tendo em vista a incerteza da caracterização desses atores como pertencentes ou não à cadeia de consumo. Por causa dessa grande insegurança jurídica, em relação às ações realizadas na rede, as empresas desmerecem o potencial econômico e de inovação dessa forma de organização das atividades empresariais, o que acaba por prejudicar não só os consumidores, mas também a si próprias. Aliás, essa ausência de regulação específica das práticas comerciais no meio digital cria também vários pontos de tensão para as empresas, dentre os quais se destacam, por exemplo, a responsabilidade dos provedores de conteúdo e hospedagem e os contratos de termos de uso dos *sites*.

Assim, a inclusão do tema em uma reforma mais ampla, do próprio CDC, sinaliza a inevitabilidade de integração desse entre as normativas de proteção ao

[116] Dados extraídos de: <http://idgnow.uol.com.br/internet/2012/01/25/defensoria-publica-do-rio-notifica-sites-de-compras-coletivas-e-vendas-online/>. Acesso em 19 de julho de 2012.

consumidor e as práticas que vão se consolidando no comércio eletrônico, que representam fatia cada vez maior do mercado de consumo.

No que tange ao âmbito do Mercosul, em dezembro, o então ministro da Ciência e Tecnologia, Aloizio Mercadante, anunciou que o bloco está preparando uma regulação comum para o comércio eletrônico[117], buscando incentivar a eficiência do livre comércio entre os países do bloco, não só nas transações entre fronterias físicas, mas, também, em meio virtual, promovendo segurança jurídica para tal. Uma das formas de atuação será o oferecimento de cursos sobre comércio eletrônico pela Escola Virtual do Mercosul[118], projeto que integra o Mercosul Digital.[119] Esse projeto é uma parceria entre o bloco latino e a União Europeia, o qual visa promover a integração econômica do bloco a partir dos desafios impostos pela Sociedade da Informação, reduzindo assimetrias tecnológicas e promovendo políticas comuns de desenvolvimento das tecnologias de informação e comunicação, sendo um dos focos do projeto, o comércio eletrônico.

7.2 Regulamentação do comércio eletrônico em 2011

Em pesquisa realizada no *site* da Câmara dos Deputados com os termos "comércio eletrônico", "*e-commerce*" ou "*ecommerce*"[120], é possível encontrar cinco projetos de lei apresentados no ano de 2011; em contraste, cada ano anterior desde 1999 apresentou apenas dois ou menos projetos de lei dessa matéria. É possível observar, portanto, que no ano de 2011 houve um aumento nas preocupações quanto à regulamentação do comércio eletrônico, o que condiz com a expansão do setor nos últimos dois anos.

---

[117] Informação retirada da notícia: <http://g1.globo.com/tecnologia/noticia/2011/12/mercosul-prepara-regulacao-comum-para-comercio-eletronico.html>. Acesso em 7 de março de 2012.

[118] No início de 2012 já era possível encontrar informações detalhadas sobre os cursos, no *site* do Escola Virtual do Mercosul: <http://www.metaanalise.com.br/inteligenciademercado/index.php?option=com_content&view=article&id=6356:escola-virtual-do-mercosul-cursos-de-comercio-eletronico&catid=8:carreira&Itemid=358>. Acesso em 7 de março de 2012.

[119] Disponível em: <http://www.mercosuldigital.org/>. Acesso em 7 de março de 2012.

[120] Disponível em: <http://www.camara.gov.br/sileg/Prop_lista.asp?formulario=formPesquisaPorAssunto&Ass1=com%C3%A9rcio+eletr%C3%B4nico&co1=+OR+&Ass2=e-commerce&co2=+OR+&Ass32=ecommerce&Submit2=Pesquisar&sigla=&Numero=&Ano=&Autor=&Relator=&dtInicio=&dtFim=&Comissao=&Situacao=&OrgaoOrigem=todos>. Acesso em 7 de março de 2012.

Dois dos projetos de lei buscam a obrigatoriedade de informação dos dados da empresa que comercializa produtos pela Internet (número no Cadastro Nacional da Pessoa Jurídica – CNPJ, endereço e telefone de suas instalações físicas) – são eles o PL nº 2.367/2011 e o PL nº 1.232/2011. Como justificativa, afirmam que, em muitos dos casos em que existem problemas quanto à compra efetuada, a ausência de informações sobre a empresa dificulta a reclamação pelo consumidor, a apresentação de queixa aos órgãos de defesa do consumidor e a demanda judicial, a qual depende do nome ou do endereço da pessoa jurídica.

O PL nº 2.096/2011, por outro lado, "visa incluir a obrigatoriedade de afixação de preços de produtos e serviços para o comércio eletrônico". Demonstra, assim, uma segunda preocupação quanto à atuação dos *sites* de *e-commerce* relativa à informação fornecida ao consumidor e vinculação à oferta.

Dois dos projetos apresentados referem-se especificamente à regulação de compras coletivas no meio eletrônico – o PL nº 1.933/2011 e o PL nº 1.232/2011, que serão relatados de forma mais detalhada no tópico a seguir.

7.3 Regulamentação das compras coletivas em 2011

As compras coletivas pela Internet são um novo tipo de comércio eletrônico, que passou por um rápido processo de expansão no mercado brasileiro nos dois últimos anos – só nesse tempo foram criados mais de 2 mil *sites* de compra coletiva no Brasil.[121] Ao mesmo tempo que evidenciou seu potencial econômico – de ofertas atrativas por preços em conta, dada a coletividade de consumidores aderindo a mesma oferta – trouxe um consequente crescimento das reclamações e potenciais violações a direitos do consumidor. Por exemplo, no Procon do Rio de Janeiro, o número de reclamações sobre *sites* de compra coletiva aumentou sete vezes em 2011 (de 49 em 2010 para 353).[122]

A grande quantidade de queixas não passou despercebida aos olhos do Legislativo do Estado do Rio de Janeiro. Em 18 de novembro de 2011, o Estado foi pioneiro na regulamentação das compras coletivas ao apresentar o Projeto de

[121] Dado retirado da notícia: <http://www.tiinside.com.br/13/02/2012/rio-sai-na-frente-e-cria-lei-para-sites-de-compras-coletivas/ti/262358/news.aspx>. Acesso em 6 de março de 2012.

[122] Dados retirados da notícia: <http://www.proteste.org.br/consumidor/rio-eeacute-pioneiro-em-lei-para-compra-coletiva-s566811.htm>. Acesso em 6 de março de 2012.

Lei de Compras Coletivas, PL nº 1.062/2011, que "estabelece parâmetros para o comércio coletivo de produtos e serviços através de sítios eletrônicos no âmbito do Estado do Rio de Janeiro".[123]

Foi destaque em 2011 também um Projeto de Lei Federal nº 1.232/2011, apresentado à Câmara dos Deputados no dia 4 de maio – o PL nº 1.232/2011[124], que busca regulamentar as compras coletivas no país. O texto do projeto de lei federal em muito se assemelha ao texto do PL do Rio de Janeiro, com a diferença de o primeiro atribuir um prazo mínimo de seis meses para utilização da oferta comprada no *site*, enquanto o segundo atribui prazo de três meses. Uma segunda diferença consiste na exigência do projeto federal de que os *sites* sejam hospedados em plataformas pertencentes a empresas com sede ou filial localizadas em território nacional – objetivando, dessa forma, a facilitação de comunicação entre o consumidor e a empresa, em casos de problemas após a compra do produto ou contratação do serviço.

Ademais, o PL do Rio de Janeiro afirma que o descumprimento do contrato de compra e venda gera "obrigações para a empresa de compras coletivas ou para a empresa responsável pela oferta do produto ou do serviço" (art. 7º), sem definir, porém, quais são essas obrigações, enquanto o Projeto de Lei Federal determina que há responsabilidade solidária entre ambas as empresas pela veracidade das informações e por eventuais danos causados ao consumidor.

Em resposta, no mesmo ano, o setor lançou um Código de Ética com o fim de estabelecer regras para as empresas de compras coletivas e fazer frente às propostas legislativas. A iniciativa[125] foi do Comitê de Compras Coletivas da Câmara Brasileira de Comércio Eletrônico, que reúne as principais empresas do setor, as quais respondem por 85% do volume total. O Código estabelece regras de boas práticas em compras coletivas e veda práticas tais como a realização de ofertas falsas, a manipulação dos contadores das compras com o fim de influenciar os usuários sobre o sucesso da oferta, bem como estabelece meios mais claros de uso de dados dos consumidores *opt-in/out*. As entidades que atenderem o Código receberão um selo de excelência.

---

[123] Cabe ressaltar que esse projeto foi aprovado e entrou em vigor no dia 9 de janeiro de 2012, sob a nomenclatura de Lei nº 6.161/2012.

[124] Disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=500481>. Acesso em 6 de março de 2012.

[125] Disponível em: <http://www.camara-e.net/Compras-Coletivas/etica/codigo-de-etica-em-compras-coletivas.pdf>. Acesso em 19 de julho de 2012.

7.4 Guerra fiscal no comércio eletrônico

No dia 1º de abril de 2011, foi publicado pelo Confaz[126] – Conselho Nacional de Política Fazendária – o Protocolo ICMS nº 21[127], buscando beneficiar os estados subscritores quanto ao recebimento de parcela do imposto relativo a produtos "cuja aquisição ocorrer de forma não presencial no estabelecimento remetente"[128]. Foi uma tentativa dos Estados de arrecadar parte dos impostos gerados pelos bilhões que estão sendo movimentados em compras pela Internet. Adquirir parte dos frutos gerados pelo comércio eletrônico se torna cada vez mais atraente, devido à facilidade e à comodidade das transações, inovação e diferenciação de ofertas, atraindo públicos diversificados e a possibilidade de prática de preços inferiores em virtude de cortes de gastos em vários fatores de formação de preços.

A justificativa para a guerra fiscal no comércio eletrônico provém das mudanças sociais e das evoluções tecnológicas que não puderam ser previstas pelo texto constitucional e, consequentemente, pelas normas infraconstitucionais aplicadas às relações consumistas. A Constituição Federal determina que, nos casos em que o destinatário do produto for o consumidor final (como no comércio eletrônico), todo o valor por ele pago a título de ICMS deverá ser arrecadado pelo Estado de origem daquele produto. Por outro lado, nos casos em que o destinatário é, por exemplo, uma loja, que revenderá o produto, o Estado de localização da loja arrecadará parte do imposto. Essa é uma das razões para os baixos preços dos produtos vendidos na rede.

Em vista da alta atratividade fiscal do comércio eletrônico e do domínio dos estados do Sul e Sudeste sobre esse ramo, os demais Estados passaram a demandar alterações de políticas fiscais para adequação da arrecadação tributária sobre mercadorias e serviços à nova realidade de transação mercadológica possibilitada

---

[126] Segundo o art. 155, §2º, XII, g da CR, cabe à lei complementar regular como os Estados e o Distrito Federal receberão benefícios fiscais, segundo sua própria deliberação. A Lei Complementar correspondente a tal disposição é a de nº 24/75, que, recepcionada pelo disposto no §8º do art. 34 do ADCT, determina que as isenções e benefícios relativos a ICMS devem ser instituídos por convênio celebrado e ratificado pelos Estados e pelo Distrito Federal. O órgão responsável por tais convênios é o Confaz, formado por um representante de cada Estado, um do Distrito Federal e um da União.

[127] Disponível em: <http://www.fazenda.gov.br/confaz/confaz/protocolos/icms/2011/pt021_11.htm>. Acesso em 8 de março de 2012.

[128] Retirado do preâmbulo do Protocolo 21: "Estabelece disciplina relacionada à exigência do ICMS nas operações interestaduais que destinem mercadoria ou bem a consumidor final, cuja aquisição ocorrer de forma não presencial no estabelecimento remetente".

pela Internet. Sem a existência dos benefícios trazidos pelo Protocolo do Confaz, os demais Estados alegam que teriam sua economia local e o desenvolvimento da região mais prejudicados do que o de costume. Ademais, alegam que o ICMS é imposto sobre consumo e, portanto, deveria haver uma repartição da arrecadação do imposto entre Estado de origem e de destino, o que é previsto pela cláusula primeira do Protocolo.[129] Essas disposições seriam apenas relativas a produtos adquiridos de forma não presencial por meio de Internet, *telemarketing* ou *showroom*.

O problema gerado por essa disputa entre Estados é a possibilidade de bitributação de produtos – Estados como a Bahia têm editado leis que obrigam o consumidor a pagar uma taxa extra de ICMS na entrega, para que não fique retido na Secretaria da Fazenda do Estado.[130] Essa sobretaxa é cobrada, entretanto, sem que o valor seja abatido do ICMS já incorporado ao preço do produto na hora da compra. No decorrer da guerra fiscal entre os Estados, quem acaba sendo prejudicado é o consumidor, que pode tanto ser compelido a pagar mais como pode estar sujeito a problemas na entrega.

A bitributação sofreu críticas de instituições como o Idec (Instituto Brasileiro de Defesa do Consumidor) e a OAB. Essa última, inclusive, ajuizou uma ação direta de inconstitucionalidade (ADI) contra o Protocolo do Confaz. Na ação, a OAB afirma que, embora a Constituição preveja a autonomia dos Estados para regular questões relativas a ICMS, deveria prevalecer a regra específica de ser feita a cobrança do imposto apenas na origem do produto, quando o destinatário é o consumidor final, de forma que este não seja onerado duas vezes.

---

[129] "Cláusula primeira. Acordam as unidades federadas signatárias deste protocolo a exigir, nos termos nele previstos, a favor da unidade federada de destino da mercadoria ou bem, a parcela do Imposto sobre Operações Relativas à Circulação de Mercadorias e sobre Prestações de Serviços de Transporte Interestadual e Intermunicipal e de Comunicação – ICMS – devida na operação interestadual em que o consumidor final adquire mercadoria ou bem de forma não presencial por meio de Internet, telemarketing ou showroom".

[130] Retirado da notícia: <http://economia.ig.com.br/estados+declaram+guerra+por+impostos+do+comercio+eletronico/n1238157416089.html>. Acesso em 8 de março de 2012.

8

Acesso, infraestrutura e arquitetura

8.1 O Plano Nacional de Banda Larga

A alta velocidade de conexão em caráter contínuo, que caracteriza a Internet banda larga, é uma garantia de acesso adequado fundamental. A infraestrutura de acesso à Internet banda larga é uma das principais ferramentas para o desenvolvimento social e econômico, uma vez que proporciona maior qualidade do serviço de Internet, permitindo inovações na rede. Quando disponibilizada em larga escala, atende às demandas de diferentes usuários – governo, setor privado e cidadãos.

Entretanto, a Internet banda larga ainda é muito restrita e pouco difundida pelo território nacional. Dentre uma população de 191,5 milhões de brasileiros[131], no início de 2011 havia apenas 16 milhões de acessos banda larga fixos e 28 milhões de acessos banda larga móvel.[132] Embora os dados sejam crescentes, ainda há a necessidade de rápida expansão da banda larga, uma vez que diversos

[131] Dados retirados da Avaliação do Diagnóstico realizado pelo Ipea sobre *A Situação da Banda Larga no Brasil*, feito pela Associação Brasileira de Telecomunicações (Telebrasil). Disponível em: <http://www.telebrasil.org.br/pnbl_sinditelebrasil_teleco_situacao_banda_larga_no_brasil.pdf>. Acesso em 4 de junho de 2012.

[132] Dados retirados do Relatório Técnico/Consultoria Análise de Utilização do Espectro de 700 MHz, da Associação Brasileira de Telecomunicações (Telebrasil). Disponível em: <http://www.telebrasil.org.br/analise_de_utilizacao_do_espectro_parte1.pdf>. Acesso em 4 de junho de 2012.

países já vem implementando planos nesse sentido[133], fazendo com que o Brasil figure situação de desvantagem se não tomar nenhuma providência.

Tendo em vista as "graves desigualdades existentes hoje no que diz respeito às condições de acesso à banda larga no país"[134], o governo lançou, no dia 5 de maio de 2010, um plano de atuação, chamado **Programa Nacional de Banda Larga** (PNBL)[135], através do Decreto 7.175/2010.[136] Esse plano pretende massificar o acesso até 2014 – o que foi definido, a princípio, como o alcance de 40 milhões de domicílios, partindo de um contexto em que apenas 11,9 milhões tinham acesso à infraestrutura de banda larga. Esse número, entretanto, foi modificado com o lançamento feito pelo Ministério das Comunicações de um segundo documento, chamado **Plano Nacional de Banda Larga**[137], o qual estabeleceu metas mais detalhadas de atuação e trouxe novidades quanto aos principais agentes do plano, conforme será visto mais adiante.

O PNBL passou a ter como metas, portanto, o alcance de 30 milhões de acessos a banda larga fixa e 60 milhões a banda larga móvel (urbanos e rurais) até 2014, além de levar acesso banda larga a 100% dos órgãos de governo e de aumentar em até dez vezes a velocidade mínima dos serviços de acesso à banda larga fixa (critério de qualidade do serviço). Estimou que seria necessário R$ 49 bilhões em investimentos (privados, públicos e por meio de linhas de crédito, como a do BNDES) para que tais metas fossem cumpridas.

---

[133] "Pelo potencial de dinamizar a economia, programas nacionais de expansão da banda larga foram adotados por vários países em seus pacotes de estímulo à recuperação econômica após crise mundial de 2008 [8]. Estados Unidos, Grã-Bretanha, Canadá, Alemanha, Portugal, Itália e Finlândia incluíram medidas explícitas neste sentido. Em ações distintas, Austrália, França, Irlanda, Japão, Cingapura e Coreia do Sul também anunciaram melhorias e expansões de sua infraestrutura de banda larga. Para citar um país latino-americano, o Chile possui um plano de ação que, dentre as diversas áreas de ação, estabelece metas de cobertura de conexões em banda larga [10]". PNBL, pág. 23.

[134] Carta publicada no lançamento do PNBL. Disponível em: <http://campanhabandalarga.org.br/index.php/2011/01/20/40/>. Acesso em 11 de julho de 2012.

[135] Disponível em: <http://www.google.com.br/url?sa=t&rct=j&q=plano%20nacional%20de%20banda%20larga%20download&source=web&cd=3&ved=0CGYQFjAC&url=http%3A%2F%2Fwww.governoeletronico.gov.br%2Fanexos%2Fplano-nacional-de-banda-larga%2Fdownload&ei=QHD0T4_1ElGg8QSLiPnqBg&usg=AFQjCNHK78IA39qh-TjnwT92Ngk9yM-IBQ>. Acesso em 04 de julho de 2012.

[136] Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2010/Decreto/D7175.htm>. Acesso em 13 de julho de 2012.

[137] Disponível em: <http://www.google.com.br/url?sa=t&rct=j&q=plano%20nacional%20de%20banda%20larga%20pdf&source=web&cd=3&ved=0CFsQFjAC&url=http%3A%2F%2Fwww.governoeletronico.gov.br%2Fanexos%2Fplano-nacional-de-banda-larga%2Fdownload&ei=TpIAUKKKOoHb6wH596SNBw&usg=AFQjCNHK78IA39qh-TjnwT92Ngk9yM-IBQ>. Acesso em 13 de julho de 2012.

Embora esse documento não tenha como intenção estabelecer valores numéricos específicos para a velocidade de banda larga adequada (preocupando-se simplesmente em garantir que a infraestrutura de Internet banda larga supra as necessidades derivadas dos seus consumidores e fornecedores de serviços), um dos principais objetivos do Programa Nacional de Banda Larga era disponibilizar planos populares de 512 a 784 Kbps por R$ 35,00. Com a intervenção do governo Dilma Roussef, essa velocidade subiu para 1 Mbps – o que equivale a duas horas e quarenta minutos de espera para baixar um arquivo de 1,2 Gb.[138]

8.1.1 Termos de Compromisso

Os planos de banda larga popular previstos pelo PNBL foram concretizados, em um primeiro momento, nos Termos de Compromisso firmados entre o Ministério das Comunicações e a Anatel com as principais concessionárias de telefonia fixa (Telefonica, Oi, Companhia de Telecomunicações do Brasil Central – CTBC e Sercomtel) em 30 de junho de 2011.[139] Como estavam sendo tratados em regime privado (impossibilitando o Estado de impor preços ou metas de ampliação do serviço), os planos populares derivaram da revisão quinquenal do contrato de concessão e da edição do novo Plano Geral de Metas de Universalização.[140] Eles preveem, ainda, que as empresas devem cobrar R$ 29,90 nas localidades em que houver isenção de ICMS.

Esses Termos de Compromisso, contudo, possuem peculiaridades que foram alvo de severas críticas.[141] Primeiro, o próprio fato de serem acordos que estabelecem

---

[138] Disponível em: <http://g1.globo.com/tecnologia/noticia/2011/06/entenda-o-plano-nacional-de-banda-larga.html>. Acesso em 13 de julho de 2012.

[139] O Ministério das Comunicações disponibiliza a íntegra dos termos neste endereço: <http://www.mc.gov.br/acoes-e-programas/programa-nacional-de-banda-larga-pnbl/252-temas/programa-nacional-de-banda-larga-pnbl/23723-termos-de-compromisso>. Acesso em 13 de julho de 2012.

[140] Também datado de 30 de junho de 2011, o PGMU III estabelece que "A Agência Nacional de Telecomunicações – Anatel deverá adotar, até 31 de outubro de 2011, as medidas regulatórias necessárias para estabelecer padrões de qualidade para serviços de telecomunicações que suportam o acesso à Internet em banda larga, definindo, entre outros, parâmetros de velocidade efetiva de conexão mínima e média, de disponibilidade do serviço, bem como regras de publicidade e transparência que permitam a aferição da qualidade percebida pelos usuários". Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Decreto/D7512.htm>. Acesso em 13 de julho de 2012.

[141] Como exemplo, destaca-se a Campanha Banda Larga é um Direito Seu!, a qual reúne uma série de instituições que defendem uma Internet barata e de qualidade para todos. Como forma de atuação, desenvolveram um Manifesto, que pode ser assinado, por qualquer um, reivindicando que a banda larga seja tratada como serviço essencial, em regime público, de maneira a garantir a igualdade entre provedores e o ingresso sustentável de novos agentes. O Manifesto pode ser encontrado neste link: <http://campanhabandalarga.org.br/index.php/manifesto/>. Acesso em 13 de julho de 2012.

um tratamento privado do serviço de banda larga representaria uma impossibilidade do governo de atuar em defesa direta dos interesses da população. Isso é, o Estado estaria sujeito aos termos contratados, quando, na verdade, deveria possuir um papel ativo como agente econômico e executor desse serviço – até mesmo para que possa alcançar a meta de massificação da infraestrutura de banda larga.

Haveria um problema quanto ao limite de *downloads* imposto nos planos populares, já que, quando ultrapassado, permitiria às concessionárias diminuir temporariamente a velocidade da Internet contratada (sem, contudo, impedir a fruição pelo consumidor das aplicações básicas), limitando, assim, o pleno uso da Internet pelo consumidor. Tal medida aparentaria uma tentativa das empresas de telecomunicações de tornar esses planos menos atraentes para o consumidor – além de não representar bons padrões de qualidade, já que a maior franquia, de 1 Gb, seria rapidamente atingida, dada que as aplicações *on-line*, hospedagem na nuvem e o consumo de vídeo *on-line* tem tornado as demandas por banda cada vez maiores. Segundo pesquisa feita pelo Idec, a União Internacional de Telecomunicações afirmou que uma banda larga de qualidade deveria ter, no mínimo, 1,5 Mbps de capacidade de *download*.[142] Além disso, o consumidor que aderir a esses planos também terá sua capacidade de *upload* muito limitada: de até 128 Kbps, o que corresponde a pouco mais que duas vezes a velocidade de uma conexão em linha discada.[143]

Ademais, os acordos obrigam as concessionárias a atuarem apenas nas "localidades sedes de municípios", o que aparentemente não inclui nem as áreas urbanas de forma ampla nem as áreas rurais. Esse fator vai de encontro com as metas gerais de universalização estabelecidas pelo Plano Nacional de Banda Larga, que afirmam que a massificação do acesso à infraestrutura de Internet banda larga deve ocorrer tanto em áreas urbanas quanto rurais, atendendo a todos os municípios do país com população superior a 100 mil habitantes.[144]

Um dos fatores que mais geraram preocupação foi a permissão, pelos Termos de Compromisso, da venda dos planos populares em conjunto com plano do servi-

---

[142] Disponível em: <http://www.idec.org.br/em-acao/revista/abertura-de-contas/materia/lenta-cara-e-para-poucos-ii-a-missao/pagina/109>. Acesso em 16 de julho de 2012.

[143] A Internet com conexão em linha discada apresenta no máximo 56,6 KBps de velocidade. Dados extraídos da *Wikipedia*: <http://pt.wikipedia.org/wiki/Linha_discada>. Acesso em 16 de julho de 2012.

[144] BRASIL. Plano Nacional de Banda Larga, p. 17.

ço de telefone fixo comutado.[145] Há a afirmação de que essa prática seria equivalente a uma venda casada entre serviço de banda larga e serviço de telefonia fixa, prática expressamente proibida pelo Código de Defesa do Consumidor.[146]

Portanto, os críticos do programa têm afirmado que a implementação destes termos representa a ausência de um plano de atuação consolidado pelo governo federal, sem contar que promoveria a massificação de um serviço de má qualidade, cujo excesso de falhas tem sido alvo de constantes reclamações pelos consumidores.[147] Segundo o Cadastro de Reclamações Fundamentadas do Procon relativo ao ano de 2011[148], "serviços mal prestados também foram alvo de reclamação em relação ao serviço de acesso à Internet por banda larga, em razão de quedas de sinal frequentes e fornecimento de velocidade inferior à contratada. Há também reclamações geradas pela falta de informação quanto aos pacotes de acesso à Internet em *roaming* internacional" (pág. 13).

As empresas de telecomunicações Telefonica e Oi, que firmaram Termos de Compromisso relativos ao PNBL, obtiveram péssimos resultados nas pesquisas apresentadas pelo relatório do Procon: ocupam respectivamente 6º e 7º lugares no *ranking* geral das cinquenta empresas mais reclamadas de 2011, além de estarem entre as cinco empresas de serviços essenciais mais reclamadas (apenas perdendo para a Tim). Interessante notar que, nessa pesquisa, o Procon também reconheceu as desvantagens que o consumidor pode sofrer com a venda casada

---

[145] Por exemplo, no Termo de Compromisso firmado com a CTBC (disponível em: <http://www.mc.gov.br/acoes-e-programas/programa-nacional-de-banda-larga-pnbl/252-temas/programa-nacional-de-banda-larga-pnbl/23723-termos-de-compromisso>), utilizaram-se os seguintes dispositivos: "§3º A hipótese prevista no §2º não isenta a ALGAR TELECOM de disponibilizar a Oferta de Varejo por meio do SCM ou com uso de tecnologia que ofereça condições técnicas de qualidade equivalentes, conforme cronograma previsto no ANEXO I, cuja contratação, neste caso, poderá ser efetuada em conjunto com plano do serviço de telefone fixo comutado – STFC disponível na respectiva localidade, na forma do §4º desta Cláusula.
§4º. Sem prejuízo do previsto no § 3º, a ALGAR TELECOM deve assegurar ao consumidor a possibilidade de contratação da Oferta de Varejo, ao preço estipulado no *caput*, combinada com o Plano Básico do STFC homologado nos termos do Anexo III ao Contrato de Concessão e, alternativamente, com ao menos um Plano Alternativo do STFC, tendo este último o preço mensal máximo de R$ 30,00 (trinta reais), com tributos, sem prejuízo da cobrança (I) pelo tráfego cursado do STFC além da franquia; (II) pela prestação de utilidades ou comodidades (PUCs); e/ou (III) por outros serviços".

[146] Art. 39. É vedado ao fornecedor de produtos ou serviços, dentre outras práticas abusivas: I – condicionar o fornecimento de produto ou de serviço ao fornecimento de outro produto ou serviço, bem como, sem justa causa, a limites quantitativos;

[147] *Sinais preocupantes: o PNBL em momento crítico*, Campanha Banda Larga é um Direito Seu!. Disponível em: <http://campanhabandalarga.org.br/index.php/2011/06/13/sinais-preocupantes-o-pnbl-em-momento-critico/>. Acesso em 16 de julho de 2012.

[148] Disponível em: <http://www.procon.sp.gov.br/pdf/acs_ranking_2011.pdf>. Acesso em 16 de julho de 2012.

entre serviços de telefonia fixa e Internet banda larga (permitida pelos Termos de Compromisso), chamando a atenção da Anatel para a necessidade de regulamentação dessa prática.[149]

8.1.2 Gestão do PNBL

De acordo com o Decreto 7.175/2010, a principal gestora do Plano Nacional de Banda Larga seria a estatal Telecomunicações Brasileiras S.A. (Telebras), a qual atuaria em conjunto com o Comitê Gestor do Programa de Inclusão Digital (CGPID), a Anatel e as empresas concessionárias de Telecomunicações. A Telebras seria responsável por implementar a rede privativa de comunicação da administração pública federal, prestar apoio e suporte a políticas públicas de conexão à Internet em banda larga para universidades, centros de pesquisa, escolas, hospitais, postos de atendimento, telecentros comunitários e outros pontos de interesse público, além de prover infraestrutura e redes de suporte a serviços de telecomunicações prestados por empresas privadas, estados, Distrito Federal, municípios e entidades sem fins lucrativos. Dessa forma, o poder público seria o principal responsável pela aplicação do Plano, tendo o setor privado papel complementar na sua implementação – sendo responsável, por exemplo, pela prestação direta do serviço de banda larga para usuários finais, a qual apenas seria substituída pela Telebras nas localidades em que não houvesse oferta adequada do serviço.

Essa divisão de tarefas entre setor público e privado, contudo, foi modificada ao longo do ano de 2011, momento em que a implantação do PNBL foi acelerada

[149] "A oferta através de pacotes, com preço e condições comparativamente mais vantajosos do que a aquisição isolada de um só serviço, desestimula a contratação individual. Aparentemente vantajosa para os consumidores, a venda e compra dos serviços em pacotes esconde problemas que podem ser enfrentados mais tarde pelo consumidor.
No momento da contratação, normalmente realizada com uma das empresas envolvidas, as informações fornecidas não são claras: empresas prestadoras distintas, normas regulatórias específicas para cada serviço e condições especiais atreladas ao pacote. Quando o consumidor enfrenta problemas, está insatisfeito ou deseja rescindir um ou mais dos serviços, sofre o jogo de "empurra" entre as empresas e é informado sobre a incidência de multa, em razão de fidelização (TV por assinatura e telefonia móvel) e sobre a alteração no valor do serviço que permanecerá ativo.
O Procon-SP aponta para a necessidade de regulamentação pela Agência Nacional de Telecomunicações (Anatel) dos serviços convergentes, uma vez que as regras são distintas para os diferentes serviços incluídos nos pacotes, como, por exemplo, a fidelização, que é permitida em alguns serviços e vedada em outros". Pág. 12 do Cadastro de Reclamações Fundamentadas de 2011, Procon. Disponível em: <http://www.procon.sp.gov.br/pdf/acs_ranking_2011.pdf>. Acesso em 16 de julho de 2012.

pelo Ministério das Comunicações – cuja gestão foi modificada junto com a mudança do governo Lula para o governo Dilma.[150] A atuação das concessionárias de telecomunicações no PNBL foi ganhando cada vez mais destaque e, consequentemente, o papel da Telebras seria restringido, focado no desenvolvimento de *backhauls*[151]. Mesmo antes da assinatura dos Termos de Compromisso, o Ministério das Comunicações já dava sinais de que o desenvolvimento do PNBL seria apoiado na atuação das empresas de telecomunicações. Isso foi expresso no esclarecimento feito pelo Ministério à Bovespa e à CVM: "é intenção do Ministério rediscutir a atuação de mercado da Telebras, a fim de diminuir projetos isolados da empresa e canalizar esforços conjuntos com o setor privado para a expansão de redes no país e sua comercialização no atacado"[152].

O próprio Plano Nacional de Banda Larga evidencia esse entendimento, ao afirmar que um dos seus princípios "é o estímulo ao setor privado para que este invista na infraestrutura de banda larga, em regime de competição, cabendo ao Estado atuar de forma complementar (...)".[153] Somado a isso, uma série de ações políticas demonstra o efetivo afastamento de funções da Telebras relativas ao PNBL. Uma delas foi o corte de recursos no governo Dilma – enquanto o governo Lula projetou um aporte inicial de R$ 1 bilhão à Telebras até o fim de 2011 com possível suplementação de R$ 400 milhões, "o primeiro aporte, de R$ 600 milhões, foi diminuído no atual governo para R$ 316 milhões, com sucessivas reduções que acabam inviabilizando a meta do PNBL para 2011".[154]

---

[150] Em 1º de janeiro de 2011 tomou posse do cargo de ministro das Comunicações Paulo Bernardo Silva, e deixou o cargo o ex-ministro José Artur Filardi, que substituiu, em 31 de março de 2010, um dos idealizadores do PNBL, o ex-ministro Hélio Costa.

[151] "*Backhauls* são as ligações de Internet das grandes redes para os municípios, a partir do qual se distribui o sinal para as redes que chegam para prover banda larga nas residências". Site Banda Larga é um Direito Seu!, *Entidades criticam negociação do governo com as Teles*, disponível em: <http://campanhabandalarga.org.br/index.php/2011/04/25/entidades-criticam-negociacao-do-governo-com-as-teles/>. Acesso em 13 de junho de 2012.
De acordo com o Plano Nacional de Banda Larga, "com relação às restrições ao crescimento da oferta de infraestrutura banda larga, o Brasil vem atuando para superar um dos principais fatores de limitação da expansão da cobertura banda larga, ou seja, a expansão do *backhaul* a mais localidades. (…) Destaca-se a importância de garantir a oferta não discriminatória aos nós de acesso ao *backhaul*" (pág. 13).

[152] Relativo ao Ofício 561/2011/SE-MC, disponível em: <http://www.bmfbovespa.com.br/agencia/corpo.asp?origem=exibir&id=18201105030168&manchete=TELEBRAS%20(TELB)%20-%20ESCLARECIMENTOS>. Acesso em 16 de julho de 2012.

[153] BRASIL. Plano Nacional de Banda Larga, p. 11.

[154] CAMPANHA BANDA LARGA. *CUT defende o fortalecimento da Telebras*. Banda Larga é um Direito Seu! Disponível em: <http://campanhabandalarga.org.br/index.php/2011/06/06/cut-defende-fortalecimento-da-telebras/>. Acesso em 16 de julho de 2012.

Também houve suspeitas de que as demissões do então presidente da Telebras e idealizador do PNBL, Rogério Santanna (em 31 de maio de 2011), e do secretário de Telecomunicações Nelson Fujimoto, representaram um esvaziamento da Telebras e de sua função como gestora do plano. Santanna já havia feito críticas ao governo, afirmando que estaria cedendo aos interesses das concessionárias de telecomunicações, e que essa aproximação com empresas privadas não era necessária, tendo em vista que a rede com a qual atuaria a Telebras já existe (derivada de acordos feitos entre a Telebras com a Petrobras e a Eletrobras, que serão explicados mais adiante), de maneira que, dentro de cinco anos, ela começaria a ter lucro. Assim, seria preciso apenas fortalecê-la (econômica e profissionalmente) e expandir essa rede, mas que esses planos estariam inviabilizados com o contingenciamento de recursos imposto à estatal.

Por outro lado, o atual ministro das Comunicações, Paulo Bernardo, afirma que essa negociação com as empresas de telecomunicações era necessária, já que foram planejados gastos de R$ 7 bilhões para se alcançar as metas do PNBL, mas a presidente Dilma Roussef somente autorizou a liberação de R$ 1 bilhão por ano – ou seja, R$ 4 bilhões no total (se a verba de 2011 for recomposta). Para ele, o importante é cumprir as metas do plano, não importando se isso será feito através do governo ou do setor privado, e sem que isso signifique uma competição entre Telebras e as empresas de telecomunicações.[155] Já Santanna acredita que os monopólios exercidos pelas principais empresas de telecomunicações prejudicam a concorrência. Consequentemente, os consumidores dos locais não atendidos pelo serviço de banda larga, apesar de representarem uma parcela signficativa do mercado, também ficam prejudicados, uma vez que ficam à mercê dos interesses das empresas e dos Termos de Compromissos com elas firmados (os quais estabelecem, como vimos, obrigações de atuar apenas nas localidades sedes dos municípios).

Essa discussão remete a uma das maiores críticas feitas ao PNBL e ao tratamento em caráter privado do serviço de acesso à infraestrutura de banda larga: a não exigência de universalização do serviço. Segundo a campanha Banda Larga é um Direito Seu!, o acesso à banda larga deveria ser tratado como um direito fundamental e um serviço essencial, o que faria com que, obrigatoriamente, estivesse sujeito ao regime público, sendo a ele garantido, assim, características próprias

[155] Informações extraídas do Observatório do Direito à Comunicação. Disponível em: <http://www.direitoacomunicacao.org.br/content.php?option=com_content&task=view&id=7924>. Acesso em 16 de julho de 2012.

desse regime, como a universalização, controle de tarifas e retorno dos bens derivados de recursos públicos à União.

Dessa forma, seria também possível utilizar os recursos do FUST (Fundo de Universalização dos Serviços de Telecomunicações) para a implantação do PNBL, o que não é possível por ser tratado em regime privado. O FUST possui arrecadação anual de R$ 600 milhões, recolhidos sobre a receita operacional bruta de todas as empresas que operam no setor, segundo o PNBL.[156] Atualmente, a lei que dispõe sobre a aplicação dos recursos desse fundo está em processo de revisão[157] e, se aprovada pelo Congresso, permitirá que sejam utilizados para qualquer investimento em serviços de telecomunicações, prestados tanto em regime público quanto privado – incluindo os serviços de acesso à infraestrutura de banda larga. A justificativa do projeto de lei afirma que o fundo já arrecadou cerca de R$ 5 bilhões, que ainda não foram utilizados nas finalidades previstas.

Apesar de todos os esforços para retirar da Telebras a gestão do PNBL, ela tomou uma série de iniciativas no ano de 2011 para a concretização do plano. Por exemplo, contratou com a Petrobras[158] e a Eletrobras[159] o direito de utilização de suas redes de fibra óptica, sem o que seria impossível alcançar as metas de massificação previstas – contrato esse que foi objeto de questionamento por processo judicial ajuizado pelas empresas de telecomunicações no fim de novembro[160]. Além disso, entrou em acordos com as empresas Claro e Tim, as quais passaram a oferecer os planos populares de banda larga[161]. Em novembro, deu início, junto à RNP (Rede Nacional de Ensino e Pesquisa), a um projeto piloto que visa a integração de universidades e institutos tecnológicos federais em alta ve-

---

[156] BRASIL. Plano Nacional de Banda Larga, p. 27.

[157] O Projeto de Lei relativo à revisão da lei que rege o sistema de aplicação de recursos do FUST é o Projeto de Lei do Senado nº 103, de 2007. Disponível em <http://www6.senado.gov.br/mate-pdf/9415.pdf>. Acesso em 16 de julho de 2012.

[158] Sobre a contratação de uso de fibra óptica com a Petrobras: <http://www.brasil.gov.br/noticias/arquivos/2011/05/19/petrobras-cede-utilizacao-de-fibras-opticas-para-programa-nacional-de-banda-larga>. Acesso em 16 de julho de 2012.

[159] Sobre a contratação de uso de fibra óptica com a Eletrobras: <http://insight-laboratoriodeideias.blogspot.com.br/2011/07/telebras-e-eletrobras-juntas-para.html>. Acesso em 16 de julho de 2012.

[160] Teles vão à Justiça para que Telebras abra contratos firmados com Eletrobras e Petrobras, Convergência Digital. Disponível em: <http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=28479&sid=14>. Acesso em 16 de julho de 2012.

[161] Sobre a Claro: <http://oglobo.globo.com/tecnologia/claro-adere-ao-programa-de-banda-larga-do-governo-oferece-servico-r-2990-2868224>. Sobre a Tim: <http://info.abril.com.br/noticias/tecnologia-pessoal/com-tim-pnbl-tera-web-movel-por-35-reais-13072011-30.shl>. Acesso em 16 de julho de 2012.

locidade à rede acadêmica nacional[162], o qual será realizado em Tocantins e em Goiás, através da ampliação da estrutura de *backhaul* nas universidades.

8.2 Regulamento de gestão de qualidade para Internet fixa e serviço móvel

Em julho de 2010, a Anatel abriu consulta pública[163] para elaboração de um Regulamento de Gestão da Qualidade do Serviço Móvel Pessoal (RGQ-SMP), com o objetivo de atualizar o então existente Plano Geral de Metas de Qualidade (PGMQ-SMP)[164] e acrescentar novos indicadores de qualidade a serem respeitados pelas prestadoras do serviço de telefonia móvel.

Em agosto de 2011, a agência adotou o mesmo procedimento[165] para Comunicação Multimídia (RGQ-SCM). Como resultado dessas consultas, a agência aprovou no ano de 2011 dois regulamentos de Gestão de Qualidade: o RGQ-SCM e o RGQ-SMP.[166] [167]

A adoção dos Regulamentos de Gestão de Qualidade da Anatel é relevante porque estabelece padrões a serem observados pelos prestadores de serviço em relação à qualidade do serviço prestado. O não cumprimento das metas de qualidade estabelecidas pela agência, que passam a ser exigíveis a partir de novembro de 2012[168], sujeita as prestadoras a sanções.[169]

---

[162] Sobre o projeto piloto entre a Telebras e a RNP: <http://portal.rnp.br/web/rnp/imprensa/-/rutelistaconteudo/6Cal/articleId/608535/groupId/489970/templateId/TPL-IMPRENSA-RNP/isPrintable/true>. Acesso em 16 de julho de 2012.

[163] BRASIL. Agência Nacional de Telecomunicações (Anatel). Consulta Pública nº 27/2010.

[164] BRASIL. Agência Nacional de Telecomunicações (Anatel). Resolução nº 317, de 27 de setembro de 2002.

[165] BRASIL. Agência Nacional de Telecomunicações (Anatel). Consulta Pública nº 46/2011.

[166] BRASIL. Agência Nacional de Telecomunicações (Anatel). Resolução nº 574, de 28 de outubro de 2011 disponível em: <http://www.in.gov.br/visualiza/index.jsp?data=31/10/2011&jornal=1&pagina=91&totalArquivos=160>. Acesso em 29 de fevereiro de 2012.

[167] BRASIL. Agência Nacional de Telecomunicações (Anatel). Resolução nº 575, de 28 de outubro de 2011 disponível em: <http://www.anatel.gov.br/Portal/exibirPortalRedireciona.do?codigoDocumento=245894>. Acesso em 20 de julho de 2012.

[168] De acordo com o art. 46 da Resolução, as metas passam a ser exigíveis 13 (treze) meses após a aprovação do regulamento.

[169] É importante destacar que os serviços de telecomunicações são constantemente apontados como um problema pelo consumidor. Segundo o Departamento de Proteção e Defesa do Consumidor do Ministério da Justiça, os serviços de telecomunicações responderam em 2011 por 22,90% do total das reclamações feitas pelos consumidores aos Procons que fazem parte do Sindec (Sistema Nacional de Informações de Defesa do Consumidor).

No que diz respeito ao regulamento do Serviço de Comunicação Multimídia[170] (serviço de telecomunicações que suporta o acesso à Internet em banda larga), a Anatel estabeleceu metas de qualidade apenas para as prestadoras com mais de 50 mil assinantes, relativas a três tipos de indicadores: Indicadores de Reação do Assinante, Indicadores de Rede e Indicadores de Atendimento.

Nos indicadores de reação do assinante, a Anatel estabeleceu que as prestadoras de SCM devem reduzir o número de reclamações recebidas em seus canais de atendimento para uma proporção de 6% em relação ao seu número total de assinantes a partir de novembro de 2012. A partir de novembro de 2014, a proporção de reclamações deve ser reduzida para 2% do total de assinantes. De maneira semelhante, a Anatel estabeleceu indicadores de reação do assinante relativos ao número de reclamações reabertas.

A maior inovação do regulamento foi em relação aos Indicadores de Rede das prestadoras de SCM.

Veja abaixo alguns dos Indicadores de Rede aprovados pela agência:[171]

- Velocidade Instantânea: é a velocidade aferida em cada medição feita pelo *software*. O resultado não pode ser menor do que 20% da velocidade máxima contratada pelo assinante, tanto para *download* como para *upload*, em 95% das medições. A meta de 20% é válida para os primeiros doze meses, contados a partir da entrada em vigor do regulamento. Nos doze meses seguintes, será de 30% e, a partir de então, 40%.
- Velocidade Média: é o resultado da média de todas as medições realizadas no mês na rede da prestadora. A meta inicial é de 60%, nos doze primeiros meses. Nos doze meses seguintes será de 70% e, a partir de então, 80%.
- Latência Bidirecional: é o tempo em que um pacote de dados percorre a rede de um determinado ponto até seu destino e retorna à sua origem. A meta, a ser observada em 95% das medições, é de, no máximo, 80 milissegundos em conexões terrestres e 900 milissegundos em conexões por satélite.

---

[170] "O Serviço de Comunicação Multimídia é um serviço fixo de telecomunicações de interesse coletivo, prestado em âmbito nacional e internacional, no regime privado, que possibilita a oferta de capacidade de transmissão, emissão e recepção de informações multimídia, utilizando quaisquer meios, a assinantes dentro de uma área de prestação de serviço" – transcrição da definição constante no Artigo 3ª da Resolução nº 272 de 9 de agosto de 2001.

[171] Conforme veiculado pela Anatel em 31 de outubro de 2011. Disponível em: <http://www.anatel.gov.br/Portal/exibirPortalNoticias.do?acao=carregaNoticia&codigo=24110>. Acesso em 29 de fevereiro de 2012.

Indicadores de Rede equivalentes foram aprovados para as conexões de dados das prestadoras de telefonia celular, de acordo com a Resolução n° 575/2011, que aprovou o RGQ-SMP.

Através dos Regulamentos de Gestão de Qualidade, a Anatel também aprovou Indicadores de Atendimento relativos ao atendimento nos Serviços de Atendimento ao Consumidor (SAC) das empresas, aos prazos para instalação do serviço e para reparo de problemas, entre outras medidas.

No curso das consultas públicas, a agência recebeu mais de 300 contribuições para a proposta de RGQ-SMP e mais de 700 contribuições para a proposta de RGQ-SCM.

Para desenhar a proposta regulatória relativa aos Indicadores de Rede, baseou-se em experiências internacionais como a do órgão regulador britânico, que criou um código voluntário de melhores práticas[172], em regulação do órgão regulador indiano (TRAI)[173], bem como em um estudo realizado pelo Inmetro em parceria com o Comitê Gestor da Internet e a Anatel.[174]

8.3 Nomes de domínio

Cada computador em rede possui um número exclusivo, chamado de **endereço IP**, que permite a localização dos mesmos na rede, viabilizando a comunicação dos terminais. Para facilitar essa comunicação, foi criado um Sistema de Nomes de Domínio (DNS) que substituiu os números por nomes. A Internet que conhecemos e usamos hoje é a dos nomes de domínio, dos endereços dos *sites* construídos por letras, palavras, frases, nomes próprios, nomes de empresas e, até mesmo, marcas. Pode-se dizer que, atualmente, nenhum usuário se lembra de acessar *sites* por meio de combinações numéricas.

A importância dos nomes de domínios transcende a viabilização dos usuários da Internet no acesso a *sites*. Hoje, os principais debates de controle de condutas de usuários na rede se valem cada vez mais dos nomes de domínio como estru-

[172] Disponível em: <http://stakeholders.ofcom.org.uk/telecoms/codes-of-practice/broadband-speeds-cop/voluntary-codes-of-practice/>. Acesso em 29 de fevereiro de 2012.

[173] Disponível em: <http://www.dot.gov.in/Acts/legislation/6oct2006.pdf>. Acesso em 29 de fevereiro de 2012.

[174] Disponível em: <http://www.inmetro.gov.br/consumidor/produtos/banda-larga.pdf>. Acesso em 29 de fevereiro de 2012.

tura essencial de identificação dos usuários. Um exemplo disso é a imposição aos provedores de acesso à Internet pelo governo francês de bloqueio de acesso por meio de nomes de domínio. Em 30 de dezembro de 2011, o governo francês editou um decreto que obrigava os fornecedores de acesso a bloquearem *sites* de jogos *on-line* que não estiverem cadastrados na agência reguladora francesa de jogo, ARJEL. Outro bom exemplo da importância dos nomes de domínio,que também ocorreu no ano passado na França, foi o uso dos mesmos na guerra presidencial entre os partidos. O candidato do Partido Socialista Francês, François Hollande, que usa o slogan *Le changement, c'est maintenant* (A mudança é agora,) lançou seu periódico nas bancas *Libération*. No dia seguinte, aqueles que acessavam o *site* <www.lechangementcestmaintenant.fr> encontravam uma paródia do periódico do candidato *L'Hibernation* (Hibernação) e de seu *slogan Le reniement, c'est maintenant* (A negação é agora). O proprietário do registro do nome de domínio em questão é a UMP, partido rival do PS. Quando questionado sobre isso, um dos membros da direção da UMP alegou que François Hollande e sua equipe falharam na proteção do candidato na Internet.

Vemos, portanto, a essencialidade dos nomes de domínio em diversas áreas, reflexos de situações comuns cotidianas do mundo não digital. Seja a plena atuação empresarial no meio digital, seja o embate político entre candidatos a presidência.

8.3.1 Propostas de regulação do tema no Brasil

Dentre os Projetos de Lei que tramitam atualmente no Congresso Nacional, dois são propostas relativas à regulação dos registros de nomes de domínio no Brasil. A proposta mais antiga, de 2003, é de iniciativa do senador José Sarney, o PL 256 de 2003. Nele pode-se observar preocupações mais legais e menos técnicas do registro dos nomes de domínio, com definições de requisitos e condições para registro. O segundo projeto é de 2011, de autoria do deputado Cláudio Cajado, cuja maior preocupação é solucionar os problemas empresariais que circundam os nomes de domínio, sobretudo os conflitos com marcas e nomes empresariais, evitando, assim confusão e abusos do princípio do *first come-first served* que rege o sistema de nomes de domínio.

PROJETOS DE LEI SOBRE REGISTRO DE DOMÍNIO NO BRASIL E RESOLUÇÃO Nº 8/2008 CGI.BR

	PL 835/2011	PL 256/2003	Res. 8/2008
Definição	Não define	Considera-se nome de domínio o conjunto de caracteres que identifica um endereço na rede de computadores Internet.	Define-se como Domínio de Primeiro Nível, DPN, os domínios criados sob o ccTLD.br, nos quais disponibilizam-se registros de subdomínios segundo as regras estabelecidas nesta Resolução.
Aspectos do proprietário de registro	Pessoas físicas e jurídicas, legalmente representadas ou estabelecidas no Brasil, com CPF ou CNPJ regular.	Qualquer pessoa física ou jurídica, de direito público ou privado, atendidos os requisitos estabelecidos nesta lei. As pessoas físicas ou jurídicas estrangeiras que não tenham domicílio ou sede no Brasil deverão constituir procurador domiciliado no país, com poderes específicos	É permitido o registro de nome de domínio apenas para entidades que funcionem legalmente no país, profissionais liberais e pessoas físicas, conforme disposto nesta Resolução. No caso de empresas estrangeiras, poderá ser concedido o registro provisório, mediante o cumprimento das exigências descritas no art. 6º, desta Resolução.
Vedação a registro	Não são registráveis como nomes de domínio de Internet nas categorias sob o .br expressões contrárias à moral e aos bons costumes, que ofendam a honra ou imagem de pessoas ou atentem contra a liberdade de consciência, crença, culto religioso ou ideia e sentimentos dignos de respeito e veneração, e nomes próprios de pessoas físicas para os quais existam homônimos, à exceção do primeiro requerente.	I – palavras ou expressões de baixo calão ou ofensivas à moral e aos bons costumes, à dignidade das pessoas, bem como as que incentivem o crime ou a discriminação em função de origem, raça, sexo, cor ou credo; II – palavras ou expressões decorrentes de reprodução ou imitação, no todo ou em parte, ainda que com acréscimos, de nome de domínio já registrado, ou das hipóteses previstas no art. 7ª, capazes de induzir terceiros em erro; III – os nomes que o órgão ou a entidade responsável pelo registro de nomes do domínio considerarem prejudiciais à conveniência, segurança ou confiabilidade do tráfego de informações na rede Internet.	O requerente declarar-se-á ciente de que não poderá ser escolhido nome que desrespeite a legislação em vigor, que induza terceiros a erro, que viole direitos de terceiros, que represente conceitos predefinidos na rede Internet, que represente palavras de baixo calão ou abusivas, que simbolize siglas de estados, ministérios, ou que incida em outras vedações que porventura venham a ser definidas pelo CGI.br.

PROJETOS DE LEI SOBRE REGISTRO DE DOMÍNIO NO BRASIL E RESOLUÇÃO Nº 8/2008 CGI.BR

continuação >

	PL 835/2011	PL 256/2003	Res. 8/2008
Requisitos	Não cause confusão com: I – marca depositada junto ao Instituto Nacional de propriedade Intelectual que não seja de titularidade do solicitante; II – título de estabelecimento, nome empresarial, nome civil, nome de família, pseudônimo ou apelido notoriamente conhecido, nome artístico singular ou coletivo, título de obra intelectual protegida ou outro nome de domínio que não seja de titularidade do solicitante ou para cujo registro não haja consentimento ou patronímico, o do titular, herdeiros ou sucessores; III – nome de pessoas jurídicas de direito público interno ou externo, excetuados os casos em que o solicitante seja um legítimo representante dessas pessoas jurídicas; IV – nome, prêmio ou símbolo de evento esportivo, artístico, cultural, social, político, econômico ou técnico, oficial ou oficialmente reconhecido, salvo quando o solicitante for o promotor do evento; V – marca notoriamente conhecida em seu ramo de atividade, nos termos da Convenção da União de Paris para Proteção da Propriedade Industrial, ainda que não esteja depositada ou registrada no Brasil.	I – a inexistência de registro prévio do mesmo nome no mesmo domínio de primeiro nível; II – a não configuração como nome não registrável, nos termos do art. 6º desta lei; III – a comprovação da titularidade ou do legítimo interesse.	Um nome de domínio escolhido para registro sob um determinado DPN, considerando-se somente sua parte distintiva mais específica, deve: I. ter no mínimo 2 (dois) e no máximo 26 (vinte e seis) caracteres; II. ser uma combinação de letras e números [a-z; 0-9], hífen [-] e os seguintes caracteres acentuados [à, á, â, ã, é, ê, í, ó, ô, õ, ú, ü, ç]; III. Não ser constituído somente de números e não iniciar ou terminar por hífen; IV. o domínio escolhido pelo requerente não deve tipificar nome não registrável. Entende-se por nomes não registráveis aqueles descritos no § único do artigo 1º, desta Resolução.

PROJETOS DE LEI SOBRE REGISTRO DE DOMÍNIO NO BRASIL E RESOLUÇÃO Nº 8/2008 CGI.BR

continuação >	PL 835/2011	PL 256/2003	Res. 8/2008
Cancelamento do registro	Não prevê	I – renúncia expressa de seu titular; II – prescrição; III – nulidade do registro; IV – perda da condição de titular ou legítimo interessado, nas hipóteses do art. 7º; V – ordem judicial	I. pela renúncia expressa do respectivo titular, por meio de documentação hábil exigida pelo NIC.br; II. pelo não pagamento dos valores referentes à manutenção do domínio, nos prazos estipulados pelo NIC.br; III. por ordem judicial; IV. pela constatação de irregularidades nos dados cadastrais da entidade, descritas no art. 4º, inciso I, alíneas "a" e "b", itens 1 e 2, após constatada a não solução tempestiva dessas irregularidades, uma vez solicitada sua correção pelo NIC.br; V. pelo descumprimento do compromisso estabelecido no documento mencionado no inciso IV, do art. 6º, desta Resolução.

8.3.2 O debate internacional

A partir de 12 de janeiro de 2012, os sufixos de endereços de *sites* na Internet não estarão mais limitados aos sufixos de países e aos tradicionais .com, .gov, .net, .org e outros mais. A *Internet Corporation for Assigned Names and Numbers* (ICANN), responsável pela supervisão dos nomes de domínio na Internet, aprovou a ampliação dos sufixos de endereços na Internet. O anúncio foi feito no início da 41ª reunião da entidade que terminou no dia 24 de junho em Cingapura.

A medida foi o principal ponto discutido na reunião. A expectativa é que grandes empresas sejam as primeiras a registrar novos domínios para as suas marcas. As novas taxas de registro custarão US$ 185 mil e o alto custo é visto pela ICANN como um fator que reduzirá o número de registros fraudulentos. Foi uma prática muito recorrente, no início do uso da Internet, o registro de nomes de domínio

de marcas por pessoas sem qualquer relação com as mesmas. O incentivo era vender o nome de domínio aos proprietários legítimos das marcas. Tal prática foi apelidada de Nova Corrida ao Ouro da era digital. A ICANN e a OMPI, em 1999, redigiram uma Política Uniforme para os nomes de domínio que prevê um mecanismo de solução de conflitos.

O alto valor das taxas cobradas é um fator de tensão entre os atores envolvidos, fomentando diversos debates e interpretações acerca do real objetivo da ICANN. Para muitos, além de reduzir os registros fraudulentos, as altas taxas cobradas servirão também para afastar pequenas e médias empresas, criando uma espécie de hierarquização entre nomes de domínio que é contrária às práticas e expectativas da Internet. Outra constante observação é a de que, com a medida, a ICANN veio praticamente a **imprimir dinheiro** para os registradores e para si mesma: a corrida para o registro dos sufixos fundamentais para o posicionamento da marca por diversas empresas, bem como as necessárias reservas contra uso indevido dos mesmos por terceiros, são um novo mercado a ser explorado, completamente criado por esta medida.

O lançamento dos novos domínios é apenas mais uma etapa no longo processo de aperfeiçoamento na forma como o conteúdo está endereçado na Internet. Agora será preciso verificar a legitimidade dos pedidos que serão analisados e resolver uma série de conflitos que inevitavelmente vão surgir, especialmente no que diz respeito à proteção da propriedade intelectual.

Outro ponto controvertido da nova regulamentação é a possibilidade de se opor ao registro de um domínio que afete a moralidade e a ordem pública. A diversidade cultural entre os países dificulta a adoção de parâmetros uniformes (um exemplo é a diversidade de alfabetos em vista da predominância do alfabeto ocidental) e essa medida poderá gerar conflitos envolvendo expressões que são proibidas em um certo país, mas não em outro.

8.4 O papel do NIC.br/CGI.br na implementação de soluções técnicas para a Internet no Brasil

O Comitê Gestor da Internet no Brasil (CGI.br), por meio principalmente de seu braço executivo, o Núcleo de Informação e Coordenação do Ponto BR (NIC.br), acompanha com atenção o desenvolvimento da Internet sob o ponto de vista tecnológico. Possui diversas iniciativas para monitorar ou influenciar a forma

como as tecnologias são adotadas e utilizadas pelas redes brasileiras, de forma a contribuir para que a Internet se desenvolva dentro dos mesmos princípios que a trouxeram até o ponto em que se encontra atualmente: uma rede aberta e propícia à inovação, cada vez mais universal.

Do ponto de vista tecnológico, a Internet é uma rede de alcance mundial que interliga computadores, *tablets*, celulares e uma infinidade de outros dispositivos. Na verdade, como seu nome sugere, é formada pela interconexão de um grande número de redes, mais ou menos independentes umas das outras. Tais redes são administradas por diferentes instituições, que têm objetivos diversos e usam equipamentos de vários fabricantes. Assim, a Internet só é possível porque todos os seus participantes concordam em seguir um conjunto comum de padrões tecnológicos, criados de forma aberta e colaborativa e aprovados por um processo de consenso aproximado pela IETF (Internet *Engineering Task Force*). Há literalmente milhares de padrões que definem como cada função, serviço e aplicação devem funcionar na rede.

As tecnologias usadas na Internet na prática regulam e restringem a forma como esta é utilizada e pode ter tanta influência sobre a rede quanto tem a política – no sentido mais tradicional do termo, já bastante explorado nesta obra. A característica de descentralização das operações que regem a Internet, e que possuem a tecnologia como fator agregador, também é um elemento importante na definição de políticas.

Poucos pontos da base tecnológica da Internet dependem de um controle central; por exemplo, os endereços IP, que identificam cada dispositivo, por serem únicos, ou o sistema de nomes de domínio, pela necessidade de um ponto de partida para as consultas na Internet. Esses pontos são fundamentais nas discussões sobre tecnologia da Internet e políticas públicas, uma vez que a centralização exige uma organização e uma definição de ações de distribuição e uso de recursos. Aí se enquadram os RIRs (*Regional Internet Registers*) e a ICANN (*Internet Corporation for Asigned Names and Numbers*), que gerenciam, respectivamente, os números de IP e os nomes de domínio na rede.

Ainda no que tange à capacidade de exercer influência sobre políticas, há vários fatores intrinsecamente ligados à tecnologia em si, ou à forma como é usada, que atuam nesse sentido. Abaixo, trataremos mais detalhadamente das principais iniciativas de dois dos órgãos responsáveis por oferecer soluções técnicas a alguns dos problemas enfrentados na Internet: o CGI e o NIC.br.

8.4.1 O esgotamento do IPv4 e do IPv6

O IP é a base tecnológica mais fundamental da rede, o protocolo que empresta seu nome a ela: Internet. É importante lembrar que a Internet é construída a partir da infraestrutura de telecomunicações tradicional, a mesma usada para os serviços de telefonia, rádio e TV – ainda assim, ela é normalmente muito mais flexível e barata do que os demais, já que faz uso dos recursos de forma muito mais eficiente. Isto é, no lugar de utilizar a comunicação por circuitos, que faz uma reserva antecipada dos recursos necessários para a comunicação entre emissor e receptor, a Internet utiliza a comutação de pacotes, dividindo a informação em pequenos blocos que podem ser enviados de forma independente pela rede, seguindo seu caminho até o destino final. A comunicação de pacotes garante tanto a eficiência do compartilhamento dos recursos de telecomunicações, quanto a construção de redes extremamente resilientes, que geram uma série de caminhos diferentes entre dois pontos quaisquer.

O que diferencia a Internet dos demais serviços de telecomunicações é justamente o endereço IP. O Protocolo Internet é, assim, responsável por identificar cada dispositivo conectado na rede por meio de números que chamamos de endereços, além de encapsular todos os dados que fluem através dela, agregando a eles informações suficientes para que cheguem a seus destinos. O IP faz uso dos diversos tipos de redes de telecomunicações diferentes, criando uma camada padronizada sobre a qual todos os demais protocolos e serviços da Internet funcionam.

O IPv6 é a versão mais recente do protocolo IP. Ele tem de ser implantado rapidamente na Internet, porque a versão anterior, o IPv4, não é mais capaz de suportar o crescimento da rede: não há mais endereços livres.

O NIC.br tem atuado de forma a suportar e fomentar a adoção do IPv6 no Brasil há vários anos. Em dezembro de 2007, o NIC.br começou a alocar os novos endereços. Em 2008, deu início a uma série de ações de fomento, que incluiu palestras técnicas em eventos e universidades; a construção de um *website* em português sobre o tema[175]; a criação e disponibilização de material didático, na forma de apostilas e de um curso *e-learning* sobre o assunto; a montagem de um laboratório didático e a criação de um curso gratuito, teórico e prático para os funcionários de provedores de Internet e outros sistemas autônomos; o fornecimento

[175] Trata-se do *website* <http://www.ipv6.br>. Acesso em 18 de julho de 2012.

de trânsito IPv6 gratuito; a criação de uma ferramenta de validação de *sites* IPv6 e, finalmente, a realização de estudos sobre a qualidade da infraestrutura IPv6 na Internet, dentre outros. Apenas no ano de 2011, houve 200 mil acessos ao *website* criado pelo NIC.br, e cerca de 700 técnicos foram treinados em 21 cursos práticos, realizados ao longo do ano em todas as regiões do país. Foram realizados, ainda, dois grandes eventos técnicos sobre IPv6, focados na apresentação de casos.

Além da atuação técnica, cuja ênfase foi a divulgação de informação e formação de técnicos capazes de planejar, implantar e operar o IPv6 na Internet, em 2011 o NIC.br foi o responsável por uma série de atividades de coordenação. Reuniões foram feitas entre o NIC.br e os diversos atores envolvidos, em especial operadoras de telecomunicações, provedores de acesso e provedores de conteúdo na Internet e, como resultado, foi programado um grande teste de funcionamento do protocolo para o início de 2012: a Semana IPv6. Além disso, delineou-se um cronograma para servir de base à implantação do protocolo no país, segundo o qual as operadoras de telecomunicações e os provedores devem oferecer trânsito de Internet em seus produtos corporativos em meados de 2012 e devem começar a ativar o suporte ao protocolo para usuários domésticos no início de 2013. Também para essa data é esperado que todos os *websites* brasileiros deem suporte ao protocolo.

A transição para o IPv6 é uma questão fundamental para a rede e há diversos riscos envolvidos. Um dos principais diz respeito ao uso de tecnologias destinadas a prolongar a vida do IPv4, as quais são bem conhecidas e vêm sendo usadas desde meados da década de 1990 – a principal delas é o NAT. Contudo, a possibilidade de usá-las sem prejuízo do funcionamento da rede e da preservação dos seus princípios fundamentais, como a conectividade *peer-to-peer* e a neutralidade, também já está esgotada. O uso do NAT por provedores de Internet sem a implantação concomitante do IPv6, por exemplo, pode trazer sérios prejuízos ao desenvolvimento da rede. Outro risco é a criação de um mercado negro para os IPv4 como tentativa de postergar a migração, o que pode prejudicar o controle sobre a unicidade da numeração, além de gerar confusão para a operação da Internet em si.

8.4.2 A sincronização dos elementos na rede e a Hora Legal Brasileira

Este tópico trata de duas questões simples e de fundamental importância, mas ainda pouco conhecidas e, por vezes, subvalorizadas: a sincronização dos elementos na rede e a Hora Legal Brasileira.

Existem, normalmente, registros (chamados de *logs*) detalhados sobre o funcionamento e as operações realizadas pelos equipamentos que fazem parte da infraestrutura da Internet, como os servidores e roteadores. Ao serem correlacionados, os *logs* transformam-se em material fundamental para a investigação de problemas técnicos, incidentes de segurança e mesmo crimes cibernéticos. Por conta disso, é importante que seu armazenamento corresponda a informações de tempo muito precisas e corretas. Ou seja, os dispositivos na Internet devem possuir hora certa, o que condiciona o bom funcionamento de diversas aplicações da Internet e vale para todos os tipos de equipamentos ligados à rede.

Como os computadores e outros equipamentos não têm capacidade, por si mesmos, de manter a hora certa, é necessário sincronizá-la com alguma referência externa. Para isso existe o NTP.br (*Network Time Protocol*), uma iniciativa conjunta do NIC.br e do Observatório Nacional (ON) para prover referências de tempo na Internet, sincronizadas à Hora Legal Brasileira e ao padrão mundial UTC de forma gratuita. Dentro da mesma iniciativa foi criado ainda um *website* e são realizadas ações de divulgação, como palestras em universidades e eventos técnicos. Dessa forma, o NTP.br pode ser considerado como um projeto estruturante, que colabora para que a infraestrutura da Internet funcione melhor e seja mais segura, sendo, inclusive, expressamente recomendado pelo CGI.br[176] para utilização pelas redes brasileiras.

No ano de 2011, foi realizada a renovação do acordo entre NIC.br e ON por mais cinco anos. Foi criado também um *banner* na forma de um relógio funcional, que pode ser integrado a qualquer *website* e permite que o usuário saiba a hora certa, saiba se seu micro está com a hora certa e publique o resultado no *twitter*, de forma a divulgar o NTP.br. Além disso, foram implantadas funcionalidades de criptografia no sistema e o conteúdo do *site* foi totalmente revisado.

8.4.3 Troca de tráfego – O PTTMetro

Uma das iniciativas mais importantes do NIC.br é o PTTMetro.[177] É um projeto estruturante, cujo objetivo é criar Pontos de Troca de Tráfego (PTTs) por todo o Brasil. Os PTTs são componentes da infraestrutura da Internet que permitem a

[176] O CGI.br indicou às redes brasileiras a utilização do NTP por meio da Resolução 009/2008, na forma especificada pelas orientações no *site* <http://www.ntp.br>. Acesso em 20 de julho de 2012.

[177] Gráficos de tráfego podem ser vistos no *site* <http://www.ptt.br>. Acessado em 15 de agosto de 2012.

interligação direta de muitas redes numa área geográfica restrita – geralmente uma cidade ou conurbação – de forma que elas possam trocar tráfego entre si.

Existem diversas vantagens no fato de as redes estarem diretamente interligadas por pontos centralizados: as redes e provedores menores economizam, pois deixam de pagar a seus *upstreams* o tráfego que passam a trocar diretamente com seus pares; conexões diretas implicam em velocidades maiores e, de forma geral, em uma rede mais resiliente; o tráfego local é resolvido localmente. Uma hipótese problemática que passa a ser resolvida por essa iniciativa é o caso do cidadão que, para acessar o *website* de sua prefeitura (e, portanto, fazer a transferência de um pacote de informações), depende de que esse pacote viaje por longas distâncias, muitas vezes, inclusive, por países estrangeiros, enquanto seu destino encontra-se no prédio vizinho. Isso acontece porque cidadão e prefeitura estão ligados a provedores de Internet distintos. Com os PTTs, portanto, a Internet no país passa a ser mais estruturada, além de mais barata, confiável e veloz para todos.

A iniciativa PTTMetro engloba tanto a função de fomentar e criar novos PTTs em todo o país (quando há condições técnicas favoráveis), quanto operá-los como um serviço de alta qualidade. O responsável por investir em equipamentos e operar os PTTs é o NIC.br, que normalmente conta com o apoio de outras instituições para investimentos em fibras ópticas apagadas e *datacenters*. Muitos dos PTTs existentes são fruto da colaboração da RNP (Rede Nacional de Pesquisas) com o NIC.br – em 2011, havia 18 PTTs em diversas localidades do país, o tráfego total agregado estava próximo a 70 Gbps e a quantidade de participantes únicos por volta dos 300 Sistemas Autônomos.

O PTTMetro é o PTT que mais cresce no mundo. É participante da Euro-IX, a Associação Europeia de PTTs, que hoje está ampliando sua esfera de atuação globalmente, além de ser um dos membros fundadores da recém-criada LACIX, a Associação dos PTTs da América Latina e Caribe.

8.4.4 Medição de qualidade da rede

Outra área de atuação do NIC.br é a medição da qualidade da Internet – área que, por vezes, tem sua complexidade e importância subestimadas. Isso ocorre porque não é possível auferir a qualidade da Internet simplesmente pela criação de um *website* para medir a velocidade de *download* de um arquivo pelos usuários. Inclusive, o Plano Nacional de Banda Larga, do qual tratamos no Tópico 8.1 desta obra, afirma que a velocidade de banda larga, por não ser

um critério sob o qual exista consenso, não é um bom medidor de qualidade da Internet.[178]

Logo, medir a qualidade da Internet não significa apenas medir a velocidade da banda. Há outros fatores importantes a serem considerados, como o respeito ao princípio da neutralidade da rede (tratado nesta obra no Tópico 3), a não ocorrência de *traffic shapping*, que prioriza alguns tipos de aplicações em detrimento de outros, ou ainda o respeito e completa aplicação do protocolo DNS.

Em 2011, as iniciativas para medir a qualidade da Internet no Brasil estiveram estruturadas em três frentes principais:

- Conectividade internacional;
- *Backbone* e *backhaul* brasileiros; e
- Última milha (a conexão até o usuário).

Nesse ano, o NIC.br esteve envolvido nos projetos internacionais TTM (*Test Traffic Measurements*, do Registro Regional Europeu) e Simon (Sistema de Monitoramento, do LACNIC, o Registro Regional da América Latina e Caribe). Implantou, ainda, o Samas (Sistema Automático de Medição entre *Autonomous Systems*) para aferir a qualidade do *backbone* e *backhaul* nacionais, e utilizou o Simet (Sistema de Medição de Tráfego de Última Milha) para aferir a qualidade da conectividade dos usuários. Em especial, o Simet operou com duas versões, uma simplificada com testes via *web*, outra mais completa, com *hardware* próprio desenvolvido pela entidade, num projeto piloto conjunto com o Inmetro, a Anatel e outros colaboradores. Neste último, a metodologia e os parâmetros utilizados para medir a qualidade da banda larga fixa serviu de subsídio para a elaboração da Resolução nº 574 de 28 de outubro de 2011, da Anatel.

8.4.5 CERT.br

Uma das missões do CGI.br é coordenar e integrar todas as iniciativas de serviços de Internet no Brasil, promovendo qualidade técnica, inovação e disseminação

[178] O PNBL, na pág. 24, afirma que "as definições existentes de banda larga são sempre feitas em termos de velocidade de acesso, e não há um consenso sobre que velocidade é essa. Isso pode ser explicado (I) pela dificuldade de se estabelecer padrões de tráfego que espelhem a diversidade de expectativas, comportamentos e padrões de uso dos consumidores finais e (II) pelo explosivo crescimento de tráfego, o qual torna obsoleta qualquer definição que se baseie apenas na largura de banda do acesso à Internet, exigindo constantes atualizações". Por isso que o Plano optou por não utilizar valores numéricos nessa definição, mas sim o fato de a extensão de banda larga se adequar ou não às demandas criadas pela sociedade naquele momento. Disponível em: <http://www.google.com.br/url?sa=t&rct=j&q=plano%20nacional%20de%20banda%20larga%20pdf&source=web&cd=3&ved=0CGYQFjAC&url=http%3A%2F%2Fwww.governoeletronico.gov.br%2Fanexos%2Fplano-nacional-de-banda-larga%2Fdownload&ei=Sl4IUPPfJ4GS9gTp8MShBA&usg=AFQjCNHK78IA39qh-TjnwT92Ngk9yM-IBQ>. Acesso em 19 de julho de 2012.

dos serviços ofertados. Nesse contexto, destacam-se a promoção de estudos e a recomendação de procedimentos, normas e padrões técnicos e operacionais para a segurança das redes e serviços de Internet e para a sua crescente e adequada utilização pela sociedade.

Tais atividades são desenvolvidas no âmbito do Núcleo de Informação e Coordenação do Ponto Br (NIC.br) e do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br). Conforme veremos mais detalhadamente a seguir, esses órgãos desenvolvem diversas atividades cujo objetivo estratégico é aumentar os níveis de segurança e de capacidade de tratamento de incidentes das redes conectadas à Internet no Brasil. O CERT.br possui como focos de atuação a conscientização sobre os problemas de segurança; a análise de tendências; a verificação da correlação entre eventos na Internet brasileira e o auxílio ao estabelecimento de novos CSIRTs (Grupos de Resposta a Incidentes de Segurança em Computadores) no Brasil.[179]

Incidentes de segurança

No que se refere ao tratamento de incidentes de segurança, o CERT.br é responsável por tratar as notificações, provendo a coordenação e o apoio no processo de resposta a incidentes e, quando necessário, colocando as partes envolvidas em contato. Como parte destas atividades, (I) provê suporte ao processo de recuperação e análise de ataques e de sistemas comprometidos; (II) estabelece um trabalho colaborativo com outras entidades, como outros CSIRTs, empresas, universidades, provedores de acesso e serviços Internet e *backbones*; e (III) mantêm estatísticas públicas dos incidentes tratados e das reclamações de *spam* recebidas.

Combate ao *spam*

A redução do envio de *spams* no Brasil envolve um conjunto de ações, entre elas a adoção, por Operadoras de Telecomunicações e provedores de acesso e serviços, de políticas como a de Gerência de Porta 25, recomendada pela resolução CGI.br/RES/2009/001/P do Comitê Gestor da Internet no Brasil, assim como a conscientização dos usuários sobre a necessidade de adotar uma postura mais proativa na Internet.

---

[179] Informações sobre os CSIRTs no Brasil são encontradas no *site* <http://www.cert.br/csirts/brasil/> Acessado em 15 de agosto de 2012.

De modo a fomentar a adoção das medidas pelos setores da sociedade, em 2011 foram intensificadas as discussões com operadoras de redes de banda larga e provedores de acesso à Internet, para a adoção de boas práticas para redução do *spam* saindo de redes do Brasil, sendo foco a adoção da prática denominada Gerência de Porta 25. As reuniões foram promovidas pelo CT-Spam, tendo a participação do CERT.br nas discussões e na produção do material discutido. Em novembro de 2011 foi assinado um Acordo de Cooperação pela Anatel, CGI.br, Sindicato Nacional das Empresas de Telefonia e de Serviço Móvel Celular e Pessoal (SindiTelebrasil) e Associações de Provedores de Acesso e Serviços Internet, e apoiado pelo Ministério Público e órgãos de Defesa do Consumidor para a implementação da Gerência de Porta 25.

Treinamento e conscientização

Para aumentar o número de profissionais treinados e o nível nacional de conscientização sobre os problemas de segurança na Internet, são desenvolvidas as seguintes atividades:

Produção de material

Desenvolvimento de documentação e material de conscientização para usuários de Internet:

- InternetSegura.br – reformulação do portal InternetSegura.br, de forma a torná-lo um ponto central para encontrar iniciativas na área de conscientização sobre questões de segurança, onde ONGs, empresas e entidades possam contribuir descrevendo seus projetos institucionais sobre o assunto.
- Nova versão da Cartilha de Segurança para Internet – em 2011 o CERT.br dedicou-se para gerar uma nova versão da Cartilha de Segurança para Internet. Esta nova versão, com lançamento previsto para o primeiro semestre de 2012, será ilustrada e contará com seções específicas sobre privacidade, redes sociais e tecnologias móveis.

Cursos licenciados da ***Carnegie Mellon University***

São oferecidos treinamentos na área de tratamento de incidentes de segurança, especialmente para membros de CSIRTs (Grupos de Segurança e Resposta a Incidentes) e para instituições que necessitem de auxílio para o estabelecimento de um CSIRT.

São ministrados os seguintes cursos do CERT® Program, do SEI/CMU, licenciados pelo CERT.br:

- *Fundamentals of Incident Handling*
- *Overview of Creating and Managing CSIRTs*
- *Advanced Incident Handling for Technical Staff*

Análise de tendências

Projeto *honey*TARG

Em 2011 o CERT.br reestruturou seus projetos de Análise de Tendências e Monitoramento de Ataques, de modo que tanto esforços unicamente nacionais, quanto aqueles envolvendo parceiros internacionais, fiquem abaixo de uma mesma estrutura.

Em setembro de 2011 foi formalizado junto ao "*Honeynet Project*" (http://www.honeynet.org/) o capítulo "*honeyTARG Chapter*" (http://honeytarg.cert.br/), coordenado pelo CERT.br. Esse capítulo consiste em dois Projetos que utilizam *honeypots* de baixa interatividade para a detecção de atividades maliciosas que abusem da infraestrutura de Internet, são eles: "Projeto *Honeypots* Distribuídos" e o "Projeto *SpamPots*".

Projeto *Honeypots* Distribuídos

Este projeto é hoje parte das atividades de rotina do CERT.br, sendo um termômetro sobre as atividades maliciosas no espaço Internet brasileiro. As atividades maliciosas observadas nos sensores permitem, também, a detecção de máquinas brasileiras comprometidas, cujos administradores de redes receberam notificações com conjuntos agregados de atividades maliciosas observadas vindo dessas redes.

Também foi dada continuidade ao envio de dados relativos a endereços IP e respectivos ataques direcionados aos *honeypots* para os seguintes CERTs nacionais: ArCERT (Argentina), AusCERT (Austrália), CERT Colômbia (Colômbia), JPCERT/CC (Japão), CERT-Polska (Polônia), CERT.PT (Portugal) Q-CERT (Qatar), CERT-TCC (Tunísia) e CSIRT Antel (Uruguai). Além disso, também são enviados dados para organizações que mantêm projetos para alertar administradores sobre ataques saindo de suas redes: *Team Cymru*, Projeto *Active Threat Level Analysis System* (ATLAS) e *Shadowserver Foundation*.

Projeto *SpamPots*

O objetivo deste projeto é obter, através de *honeypots* de baixa interatividade, dados relativos ao abuso da infraestrutura de Internet para o envio de *spam*. Temos hoje sensores em parceria com as seguintes instituições (por ordem de ativação do sensor): CSIRT USP (Brasil), CERT.at (Áustria), CSIRT Antel (Uruguai), SURFnet (Holanda), TWCERT (Taiwan), CLCERT (Chile), AusCERT (Austrália) e CSIRT UTPL (Ecuador). Há também um sensor mantido pelo próprio CERT.br.

Também houve continuidade no trabalho conjunto com a equipe do Laboratório e-Speed, do DCC/UFMG, para atingir o aprimoramento dos algoritmos de mineração de dados e a definição de melhores processos de análise e apresentação dos dados. No ano de 2011 o escopo da pesquisa foi expandido de modo a intensificar os esforços para detecção de *botnets* e de campanhas de *phishing*.

Os resultados acadêmicos do trabalho até o momento foram publicados em congressos científicos da área:

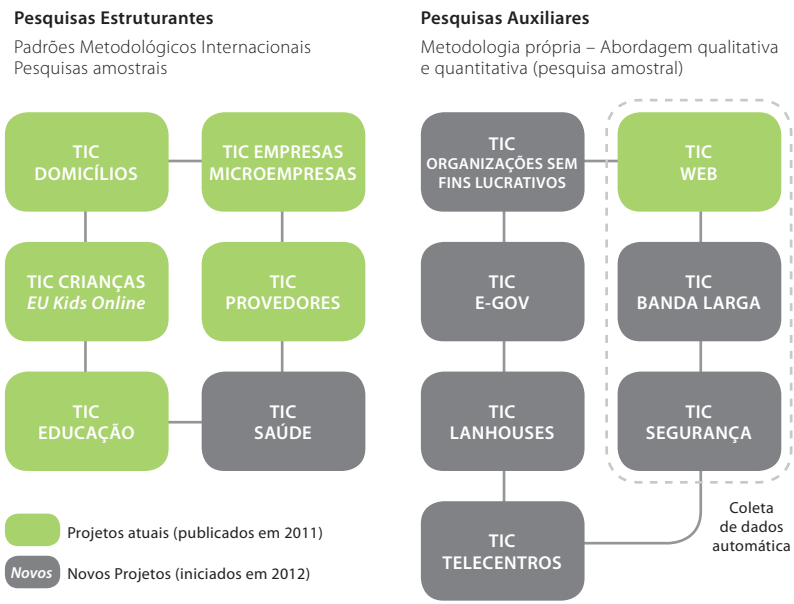
- *Spam detection using web page content: a new battleground* – Ribeiro M. T. C.; Teixeira L. V.; Veloso A. A.; Guedes Neto D. O.; Meira Junior, W.; Chaves M. H.; Steding-Jessen K.; Hoepers *C. In*: *The 8th Annual Collaboration, Electronic messaging, Anti-Abuse and Spam Conference* (CEAS 2011), 2011, Perth, Australia. *Proc. of the The 8th Annual Collaboration, Electronic messaging, Anti-Abuse and Spam Conference*, 2011. p. 83-91.
- Detecção de *Spams* Utilizando Conteúdo *Web* Associado a Mensagens – Ribeiro, M. T., Teixeira, L. V., Guerra, P. H. C., Veloso, A., Meira Jr., W., Guedes, D., Hoepers, C., Steding-Jessen, K., Chaves, M. In: XXIX Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC 2011), 2011, Campo Grande. Anais do XXIX Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC 2011). SBC, 2011. p.455 – 468.
- SpSb: um ambiente seguro para o estudo de *spambots* – Silva, G. C.; Arantes, A. C.; Steding-Jessen, K.; Hoepers, C.; Chaves, M.; Meira Jr., W.; Guedes, D.. In: Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais, 2011, Brasília. Anais do XI Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais, 2011. p. 1-5.
- Fatores que afetam o comportamento de *spammers* na rede – Silva, G. C.; Steding-Jessen, K.; Hoepers, C.; Chaves, M.; Meira Jr., W.; Guedes, D. In: Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais, 2011, Brasília. Anais do XI Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais, 2011. p. 1-14.

8.4.6 As pesquisas e análises do CGI/NIC.br sobre uso das TIC no Brasil

No contexto da missão do Comitê Gestor da Internet no Brasil – CGI.br de coordenar e integrar todas as iniciativas de serviços Internet no Brasil, promovendo a qualidade técnica, a inovação e a disseminação dos serviços ofertados, destaca-se uma de suas atribuições: a de promover a realização de pesquisas especializadas sobre o uso das tecnologias de informação e comunicação (TIC). Desta forma, o CGI.br, por meio do Núcleo de Informação e Coordenação do Ponto BR (NIC.br) e do seu Centro de Estudos sobre o uso das TIC no Brasil (CETIC.br), vem desenvolvemdo, desde 2005, pesquisas com o objetivo de produzir indicadores e estatísticas para monitorar o avanço da Internet em diversos segmentos da sociedade brasileira.

Desde a sua criação, o CETIC.br vem testemunhando o debate em torno da temática da inclusão digital no país: o discurso dos setores público e privado tem sido carregado de grande potencial transformador e de promessas de se viabilizarem políticas públicas e/ou programas de desenvolvimento nacional com vistas à transformação social e econômica. Os indicadores e estatísticas produzidos pelo CETIC.br contribuem de forma consistente não só para a produção de informação pertinente sobre a evolução do uso da rede no país, como principalmente para a análise de seu impacto no desenvolvimento socioeconômico brasileiro, resultante do debate nacional sobre a inclusão digital. Ao longo da sua existência, o CETIC.br consolidou-se como centro de referência na produção de indicadores e estatísticas sobre o uso das tecnologias de informação e comunicação e, principalmente, da Internet no Brasil. O CETIC.br vem concentrando esforços para a ampliação e melhoria da qualidade dos indicadores e das estatísticas produzidas anualmente em suas pesquisas, com o objetivo de garantir a confiabilidade dos dados, a geração de melhores informações e, sobretudo, melhor nível de comparabilidade internacional. Isto inclui a aplicação de metodologias de pesquisas quantitativas e qualitativas, baseadas em modelos e referências internacionais, tais como as referências metodológicas e de definição de instrumento de coleta de dados do *Partnership on Measuring* ICT *for Development* da ONU, documentos da Eurostat, Unesco, OECD e UNCTAD.

Esta seção tem como objetivo sintetizar os principais projetos de pesquisas conduzidos pelo CETIC.br para medição do uso das TIC em diversos segmentos da sociedade: TIC Domicílios, TIC Crianças, TIC Empresas, TIC Educação, TIC Provedores, TIC Governo Eletrônico, TIC *Lanhouses*, TIC Telecentros, TIC Organizações sem Fins Lucrativos, TIC *Web*, TIC Saúde, TIC Banda Larga e TIC Acessibilidade. A figura a seguir apresenta um resumo de todos os projetos de pesquisas do CGI.br atualmente sendo executados pelo CETIC.br .



Projeto TIC Domicílios

A Pesquisa TIC Domicílios tem o objetivo de traçar uma perspectiva completa sobre a posse e o uso das tecnologias da informação e comunicação no Brasil. Os procedimentos metodológicos adotados para a pesquisa TIC Domicílios estão baseados nas orientações da Organização para a Cooperação e Desenvolvimento Econômico (OCDE), do Instituto de Estatísticas da Comissão Europeia (Eurostat), e do Observatório para a Sociedade da Informação na América Latina e Caribe (Osilac), da Comissão Econômica para a América Latina e Caribe das Nações Unidas (Cepal).

O plano amostral da pesquisa é desenhado a partir dos parâmetros da Pesquisa Nacional por Amostras de Domicílios (PNAD), realizada anualmente pelo IBGE (Instituto Brasileiro de Geografia e Estatística), com o intuito de garantir a representatividade da amostra da população brasileira acima de 10 anos de idade. A amostra compreende 25 mil domicílios distribuídos por todo país e inclui áreas urbanas e rurais. A pesquisa tem como método de coleta de dados entrevistas presenciais, face a face, com a aplicação de questionários estruturados. Os módulos para os quais foram criados indicadores são:

- Módulo A – Acesso às tecnologias da informação e da comunicação;
- Módulo B – Uso do computador;
- Módulo C – Uso da Internet;
- Módulo G – Governo eletrônico;
- Módulo H – Comércio eletrônico;
- Módulo I – Habilidades com o computador/Internet;
- Módulo J – Acesso sem fio (uso do celular);
- Módulo K – Intenção de aquisição de equipamentos e serviços TIC.

Projeto TIC Crianças

A Pesquisa TIC Crianças tem o objetivo de traçar uma perspectiva completa sobre a posse e o uso das tecnologias da informação e comunicação no Brasil pelas novas gerações de crianças de 5 a 9 anos. A pesquisa tem como base o questionário da TIC Domicílios, que por sua vez segue o padrão metodológico da Organização para a Cooperação e Desenvolvimento Econômico (OCDE) e do Instituto de Estatísticas da Comissão Européia (Eurostat).

De modo a se assegurar a representatividade da população brasileira, a diversidade regional, econômica e social do país foi incorporada no desenho amostral por meio de cotas para determinadas variáveis. Desse modo, a amostra da pesquisa TIC é sistemática, estratificada por conglomerados e cotas no último estágio.

As entrevistas relativas à amostra principal de domicílios foram realizadas presencialmente em 2.516 residências, com indivíduos entre 5 e 9 anos de idade. A pesquisa permite a apresentação dos resultados de acordo com as seguintes variáveis de cruzamento: regiões geográficas, classe social, renda familiar, grau de instrução, faixa etária, sexo e situação de emprego. A pesquisa de campo utilizou um questionário estruturado por meio de entrevistas presenciais domiciliares (face-a-face). A entrevista contou com a presença dos pais e/ou responsáveis ao lado das crianças. Os módulos para os quais foram criados indicadores são:

- Módulo A – Acesso às tecnologias da informação e da comunicação no domicílio;
- Módulo B – Uso de computadores;
- Módulo C – Uso da Internet;
- Módulo E – Uso do e-Mail;
- Módulo I – Habilidades com o computador/Internet; e
- Módulo J – Uso do celular.

Projeto TIC Empresas

A Pesquisa TIC Empresas, tem o objetivo de produzir um retrato do uso das TIC nas empresas comerciais, compreendendo as diferenças da natureza de atuação, de porte (número de funcionários) e das cinco regiões.

O universo da pesquisa abrange as empresas com dez ou mais funcionários, pertencentes às 11 seções da CNAE – Classificação Nacional de Atividades Econômicas – propostas pela UNCTAD. A Rais – Relação Anual de Informações Sociais – serve como cadastro-base para o desenho da amostra e para a seleção das empresas, e a escolha das seções da CNAE, assim como da estrutura de porte das empresas, segue as recomendações internacionais, o que garante a comparabilidade dos dados. As entrevistas com as empresas foram feitas por telefone, utilizando questionário estruturado, com duração média de 30 minutos. O principal respondente é o responsável pela área de informática, tecnologia da informação, gerenciamento da rede de computadores ou área equivalente. Além disso, nas empresas com 250 funcionários ou mais, uma parte do questionário foi aplicada com um funcionário de área financeira, contábil ou administrativa. Os módulos para os quais foram criados indicadores são:

- Módulo A – Informações Gerais sobre os Sistemas TIC;
- Módulo B – Uso da Internet;
- Módulo C – Governo Eletrônico (e-Gov);
- Módulo E – Comércio Eletrônico;
- Módulo F – Habilidades no uso das TICs; e
- Módulo G – *Softwares*.

Projeto TIC Educação

A revolução causada pelas Tecnologias de Informação e Comunicação (TIC) tem induzido mudanças profundas, que abrangem todos os setores da sociedade, dentre eles a Educação. A adoção e uso das TIC no contexto dos sistemas educacionais tornaram-se um desafio e uma prioridade em muitos países que têm investido no uso das novas tecnologias na educação. A implantação de infraestrutura tecnológica – através de computadores de mesa, *notebooks*, televisores, câmeras e filmadoras digitais, etc. – o desenvolvimento profissional de professores e a criação de conteúdos digitais de aprendizagem são alguns exemplos desses investimentos.

A Pesquisa TIC Educação tem como objetivo identificar o uso e a apropriação do computador e Internet nas escolas públicas brasileiras através da prática

docente e gestão escolar. Além disso, o projeto busca oferecer subsídios que contribuam no desenvolvimento de ações e políticas para a apropriação das TIC nas escolas. A pesquisa conta com uma amostra de 900 escolas públicas e particulares de Ensino Fundamental e Médio em áreas urbanas em todo o território nacional. Neste sorteio de amostra foram excluídas do universo: áreas rurais, escolas federais e turmas multiseriadas.

A realização desse projeto requer a coleta de dados junto aos agentes do sistema educacional: diretores, coordenadores pedagógicos, professores (português e matemática) e alunos (5º ano do Ensino Fundamental I, 9º ano do Ensino Fundamental II e 2º ano do Ensino Médio). O método de coleta utilizado foi a aplicação de questionários estruturados através de entrevistas presenciais (face a face). Os módulos para os quais foram criados indicadores são:

- Módulo A – Perfil (diretor, coordenador pedagógico, professor, aluno);
- Módulo B – Perfil de uso do computador e Internet (diretor, coordenador pedagógico, professor e aluno);
- Módulo C1 – Atividades administrativas, planejamento e interação com a comunidade (diretor);
- Módulo C2 – Atividades de planejamento (coordenador pedagógico);
- Módulo C3 – Atividades educacionais e escolares (professor);
- Módulo C4 – Atividades escolares na Internet (aluno);
- Módulo D – Habilidades com o computador e Internet (professor e aluno);
- Módulo E – Treinamento específico (professor e aluno);
- Módulo F – Infraestrutura de TIC na escola (diretor);
- Módulo G – Barreiras ao uso (diretor, coordenador pedagógico e professor).

Projeto TIC Provedores

O avanço do processo de inclusão digital no Brasil depende diretamente do desenvolvimento e expansão da infraestrutura da Internet, sobretudo em localidades de menor atratividade de mercado. Os provedores de serviços de Internet (ISP), que incluem os provedores de acesso, de conteúdo, de hospedagem, de *e-mail* ou de aplicação, são componentes vitais para a expansão da infraestrutura da rede no país. Neste contexto, a inclusão efetiva do cidadão brasileiro na era digital depende da existência de provedores de acesso à Internet em pequenas localidades no interior do país.

Visando apresentar um panorama completo do mercado de provimento de acesso à Internet no Brasil a partir da construção de um Cadastro Nacional de

Provedores, o Comitê Gestor da Internet no Brasil (CGI.br) e o Núcleo de Informação e Coordenação do Ponto BR (NIC.br) decidiram realizar a Pesquisa TIC Provedores. Este levantamento contou com a colaboração das Associações de Provedores: Abranet, Abramulti, Abrappit, Abrint, Anid, Global Info, Internet Sul e Rede TeleSul. Os módulos para os quais foram criados indicadores são:

- Módulo A – Características gerais sobre serviços oferecidos;
- Módulo B – Infraestrutura de conexão à Internet;
- Módulo C – Informações sobre o negócio (clientes, área de atuação, velocidades oferecidas).

Projeto TIC Governo Eletrônico

Seguindo a tendência mundial de muitos governos que aderiram às tecnologias de informação e comunicação como ferramentas de modernização da administração pública, melhoria da eficiência e qualidade na prestação de serviços públicos e transparência, o governo brasileiro também vem investindo recursos na ampliação de programas de governo eletrônico (e-Gov). No entanto, para que os gestores públicos possam planejar estrategicamente a entrega de serviços de e--Gov que atendam às necessidades dos cidadãos e das empresas, é necessário que haja informação estruturada e sistemática a respeito do uso do e-Gov no Brasil.

A Pesquisa TIC Governo Eletrônico tem o objetivo de produzir indicadores e estatísticas relativas ao uso do e-Gov no Brasil. A metodologia utilizada teve duas diferentes abordagens: uma qualitativa, fazendo uso da técnica de grupos focais com cidadãos e entrevistas em profundidade com empresas; e outra quantitativa, por meio de pesquisa amostral e uso de questionários estruturados. A coleta de dados da pesquisa quantitativa é realizada junto a empresas e cidadãos em todo o território nacional. Na dimensão qualitativa desta pesquisa, procurou-se capturar aspectos profundos emergentes a partir do que os entrevistados forneceram como referências e com o significado que a estes aspectos atribuíram, dentro de uma premissa de realidade subjetiva e socialmente construída. Os módulos para os quais foram criados indicadores são:

- Módulo A – Uso da Internet;
- Módulo B – Uso de serviços públicos pela Internet;
- Módulo C – Percepções sobre governo eletrônico;
- Módulo D – Barreiras ao uso de governo eletrônico;
- Módulo E – Comunicação governo-sociedade;
- Módulo F – Variáveis contextuais.

Projeto TIC Lanhouses

As *lanhouses* constituem uma oportunidade para a participação cidadã e para o trânsito no mundo cultural, educacional e de lazer, por meio do acesso às tecnologias de informação e comunicação. Entre outros fatores, a pequena penetração do acesso à Internet nos domicílios de baixa renda criou condições para o surgimento e a expansão de estabelecimentos comerciais que oferecessem esse serviço. Em 2007, o CGI.br destacou o fenômeno das *lanhouses*, lançando luz à questão do local de acesso, dado que a maioria dos usuários de Internet brasileiros de áreas urbanas acessou a rede a partir dos centros públicos de acesso pago. A pesquisa TIC *Lanhouses* é uma iniciativa inédita conduzida pelo CGI.br que retrata as questões de gestão do negócio, a infraestrutura disponível, o perfil dos clientes e do empreendedor.

A Pesquisa TIC *Lanhouses* tem o objetivo de traçar uma perspectiva na gestão das *lanhouses* no Brasil e pode ser expresso em três grandes temas. O primeiro está relacionado com a dimensão desse setor: a quantidade de *lanhouses* no país, onde estão localizadas e quais as variáveis que interferem na sua incidência. O segundo diz respeito ao perfil desses estabelecimentos: caracterizar os estabelecimentos no que diz respeito à sua infraestrutura, modelo de negócio, sustentabilidade, entre outros indicadores. O terceiro é identificar alternativas para o futuro do segmento, tendo em vista as mudanças no perfil do acesso do brasileiro.

Para fins dessa pesquisa, define-se *lanhouse* como sendo todo estabelecimento comercial que oferece o serviço de acesso ao computador e à Internet, ainda que essa não seja sua atividade principal. A amostra da pesquisa é probabilística, estratificada, por estágios, utilizando área *sampling* e probabilidade proporcional ao tamanho (PPT) para seleção de municípios e setores censitários. As entrevistas serão presenciais, face a face, com questionário estruturado, aplicado com o proprietário ou gestor do estabelecimento. Os módulos para os quais foram criados indicadores são:

- Módulo A – Infraestrutura do estabelecimento;
- Módulo B – Modelo de negócio;
- Módulo C – Sustentabilidade;
- Módulo D – *Softwares*;
- Módulo E – Investimentos futuros;
- Módulo F – Ferramentas de gestão;
- Módulo G – Perfil do público;
- Módulo H – Perfil do gestor.

Projeto TIC Telecentros

Os telecentros constituem um importante espaço para o processo de inclusão de digital. Além de disponibilizar computadores conectados à Internet, os telecentros oferecem uma oportunidade de acesso, uso e apropriação de tecnologias digitais para solucionar problemas e contribuir para o exercício da cidadania. Não distante da perspectiva de inclusão digital, os telecentros podem ter múltiplos propósitos, como ser um espaço aberto ao público para treinamento e capacitação que oferecem facilidades de processamento e impressão de documentos, bem como outros recursos de computação. Como espaços livres, podem atender aos mais diversos perfis populacionais espalhados pelo país incluindo áreas à margem da atuação do mercado.

A Pesquisa TIC Telecentros tem o objetivo de avaliar a contribuição das políticas públicas do governo federal – Gesac, Telecentros.Br, Telecentros Comunitários – para a inclusão digital no Brasil. Os objetivos específicos da pesquisa incluem:

- Diagnosticar a situação de funcionamento de telecentros;
- Identificar fatores críticos para o funcionamento efetivo de um telecentro;
- Avaliar a contribuição dos telecentros para a promoção da inclusão digital;
- Investigar os impactos e transbordamentos socioeconômicos da implementação de um telecentro em uma comunidade local;
- Definir critérios para orientar áreas prioritárias para a instalação de telecentros;
- Sugerir melhorias para políticas públicas de inclusão digital;
- Criar uma metodologia que possa ser replicável.

O público-alvo da pesquisa é composto por telecentros, definidos como toda organização que recebeu qualquer tipo de benefício do Ministério das Comunicações para a implementação de um estabelecimento que ofereça ao público o acesso gratuito a computadores conectados à Internet.

Projeto TIC Organizações Sem Fins Lucrativos

A Pesquisa TIC Organizações sem Fins Lucrativos tem como objetivo central mapear a infraestrutura, o uso e as capacidades/habilidades acumuladas nas organizações sem fins lucrativos sobre as TIC, de forma a gerar dados que ajudem a compreender a penetração destas tecnologias, seus aportes para a gestão das instituições e possíveis benefícios para suas comunidades de atuação. Os objetivos podem ser agrupados em três grandes áreas:

- Identificar a infraestrutura de TIC nas organizações sem fins lucrativos;
- Compreender qual o uso efetivo que se faz das TIC em organizações sem fins lucrativos (tendo em vista aspectos como a captação de recursos, gestão, uso de redes sociais na Internet, mobilização e comunicação);
- Avaliar as capacidades/habilidades acumuladas pelas instituições na área de tecnologia da informação e comunicação, traduzidas nas capacidades de suas lideranças e colaboradores de fazer uso inovador das TIC.

Projeto TIC *Web*

Desde meados dos anos 90, a *web* brasileira tem mostrado acentuado crescimento, tanto no número de usuários como no leque de serviços e aplicações oferecidos por meio da rede. É flagrante o avanço de seu uso pela população brasileira: de 37 milhões de usuários, em 2005, passou a aproximadamente 65 milhões, em 2009. Igualmente impressionante é a mudança de comportamento do cidadão, que utiliza cada vez mais serviços transacionais em ambientes virtuais, conforme mostram as pesquisas do CGI.br.

O impacto do uso da Internet e da *web* na sociedade, nos indivíduos e nas organizações tornou-se objeto de pesquisa, extrapolando o campo especializado da computação aplicada, e atingindo áreas de estudos organizacionais e sociológicos. Por ser essencialmente dinâmica e sem fronteiras, tanto do ponto de vista físico como virtual, é importante que seja conhecida em detalhes, tanto para assegurar sua livre transformação quanto para permitir sua disponibilidade, confiabilidade e acessibilidade por todos.

Assim, o Comitê Gestor de Internet do Brasil – CGI.br e o Núcleo de Informação e Coordenação do Ponto Br – NIC.br, por meio do W3C Brasil e do Centro de Estudos e Pesquisas em Tecnologias de Redes e Operações – CEPTRO.br, criou mais uma iniciativa para um melhor conhecimento e entendimento da Internet brasileira: o Projeto Censo da *Web* .br. Realizado em parceria com a Secretaria de Logística e Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão (SLTi/MPOG), a Associação Brasileira de Entidades Estaduais de Tecnologia da Informação e Comunicação (ABEP) e o instituto Nacional de Ciência e Tecnologia para a *web* (inWeb), ainda com o apoio metodológico do Centro de Estudos sobre as Tecnologias de informação e Comunicação – CETiC.br, esse projeto tem como objetivo criar indicadores para contribuir para o estudo e evolução da *web* brasileira, cujo escopo é definido mais adiante.

Projeto Censo do .gov.br

Esse projeto de pesquisa enseja um primeiro esforço a fim de estabelecer a metodologia capaz de estimar o chamado "grau de cobertura" para a consequente correção das estimativas do tamanho do .gov.br. O objetivo foi definir uma estimativa para o tamanho da parte da *web* .br sob o domínio .gov.br, e em seguida fazer um levantamento de informações usando técnicas automatizadas de coleta dentro das páginas do .gov.br.

A coleta de dados sobre os domínios do governo identificou um total de 18.796 sítios sob o .gov.br, a partir de URLs percorridas. A identificação do total de sítios partiu de dados fornecidos das seguintes fontes:

- Domínios identificados como .gov.br (domínios reservados ao governo federal), cuja lista foi fornecida pela autoridade de registro para nomes de domínio no Brasil, o Registro.br, com autorização do Ministério do Planejamento, responsável pelo uso dos domínios sob o .gov.br;
- Domínios identificados como sigla-uf.gov.br, registrados pelas empresas estaduais de processamento de dados, vinculadas aos governos estaduais;
- Resultados de consultas e buscas de informações, utilizando ferramentas de busca, com o objetivo de complementar as informações anteriores.

Essas diferentes fontes foram unificadas e serviram como semente para um sistema coletor automático. Objetivou-se com esse levantamento produzir um cadastro que pudesse contemplar o maior número possível de sítios e páginas governamentais, de tal modo que fosse o mais próximo de um censo da *web* governamental brasileira.

A pesquisa TIC *Web* tem como objetivo replicar o estudo do .gov.br para todos os domínios existentes no .com.br. Devido ao tamanho da *web* do .com.br e considerando ainda os recursos de tempo, processamento, conectividade e disco necessários para coletar, armazenar e processar os dados, decidiu-se por desenvolver uma técnica de amostragem para *web*. Este projeto ainda está em fase de desenvolvimento.

Projeto TIC Saúde

Tendo como premissa o fato de que as TIC podem contribuir com o desenvolvimento das políticas públicas de saúde em suas diversas esferas, a pesquisa TIC Saúde tem o objetivo de investigar as seguintes frentes:

- Mapear a infraestrutura de TIC disponível nos estabelecimentos de saúde brasileiros (hospitais, clínicas, ambulatórios, etc.);
- Mapear as aplicações baseadas nas TIC destinadas a apoiar serviços médicos e a gestão dos estabelecimentos;
- Investigar as atividades realizadas por meio do uso de TIC e as habilidades possuídas pelos profissionais para esta utilização;
- Compreender as motivações e barreiras para a adoção e uso das TIC por profissionais de saúde (gestores e profissionais de atendimento);
- Prover uma série histórica de dados para dar suporte à formulação, implementação e avaliação de políticas públicas.

Projeto TIC Banda Larga

O cenário brasileiro de Internet é marcado atualmente por uma expansão crescente de acessos fixos de banda larga instalados: 15,5 milhões no ano de 2010, de acordo com dados da Anatel (Agência Nacional de Telecomunicações). No entanto, a prestação do serviço de banda larga hoje atinge preponderantemente os domicílios de classes sociais de mais alta renda (classes A e B) e que residem nas regiões urbanas mais rentáveis. Isto revela que a inclusão digital, sobretudo a universalização do acesso em banda larga no país, ainda é um desafio.

Por outro lado, muitos daqueles que já possuem acesso à banda larga fixa não estão satisfeitos com o serviço que contrataram. As principais reclamações dos consumidores em órgãos de proteção e defesa do consumidor relacionam-se ao elevado preço cobrado pelo serviço; à falta de viabilidade técnica para a instalação do serviço e à qualidade do serviço (interrupções e instabilidade da conecção).

O projeto de pesquisa TIC Banda Larga tem por objetivo geral medir a qualidade dos serviços de banda larga fixa nos domicílios brasileiros a partir de uma amostra em painel durante o período de seis meses a um ano. A partir dos resultados da pesquisa, pode-se verificar, por exemplo, se o serviço oferecido pelos provedores de Internet banda larga está em conformidade com o que foi contratado pelo consumidor. Além disso, os resultados poderão servir de subsídios para políticas públicas de universalização da Internet visto que apresentarão um mapa da banda larga no Brasil, identificando possíveis gargalos e áreas prioritárias de atuação. A metodologia da pesquisa é quantitativa, com uma abordagem longitudinal utilizando um painel de domicílios que possuem conexão de banda larga.

Projeto TIC Acessibilidade

A Pesquisa TIC Acessibilidade tem o objetivo de investigar questões que se configuram como barreiras para a inclusão digital e que dificultam um uso mais efetivo das redes por todos os cidadãos brasileiros e com especial atenção para pessoas com deficiência. Inicialmente, optou-se pela realização de um estudo exploratório sobre o uso da Internet entre diferentes públicos com o intuito de compreender os desafios da acessibilidade para a construção de uma Internet e *web* universal. Os objetivos específicos desta pesquisa são:

- Identificar os principais usos da Internet entre pessoas com deficiência visual, auditiva e física, crianças e usuários de computador/Internet;
- Avaliar os benefícios da Internet percebidos pelo público investigado;
- Identificar formas e experiências de aprendizagem com o uso da Internet;
- Identificar o uso, disponibilidade e forma de obtenção de tecnologias assistivas;
- Identificar barreiras e dificuldades para o uso efetivo da Internet entre pessoas com deficiências, crianças e usuários de computador/Internet.

8.4.7 A *Web* na visão do W3C Brasil

Internet e *Web* não são sinônimos. A World Wide Web, ou simplesmente *Web*, é o mais conhecido meio usado para acessar as informações disponibilizadas pela Internet. A *Web* é um conjunto de serviços que permite abrir documentos localizados em qualquer parte do mundo e por meio de hiperlinks navegar em sítios com os mais diversos conteúdos e interagir em redes sociais. Portanto, a *Web* usa a Internet como meio, mas não é a Internet em si. Tecnicamente, a Internet é uma infraestrutura em rede que conecta dispositivos globalmente, utilizando o protocolo TCP/IP para comunicação, e a *Web* é uma aplicação que usa a Internet para compartilhamento de objetos digitais – vídeos, imagens, efeitos.

A *Web* serve para expor, referenciar e vincular em rede digital. Observar a *Web* significa acompanhar como e em que condições ela cumpre o seu papel e que fatores tem se apresentado como obstáculos para que ela alcance o seu potencial máximo.

O Consórcio World Wide Web (W3C)[180] é um consórcio internacional no qual as organizações filiadas, uma equipe em tempo integral e o público trabalham

[180] Disponível em: <http://www.w3.org/>.

juntos para desenvolver padrões para a *Web*. Liderado pelo inventor da *Web* Tim Berners-Lee e o CEO Jeffrey Jaffe, o W3C tem como missão conduzir a World Wide Web para que atinja todo seu potencial, desenvolvendo protocolos e diretrizes que garantam seu crescimento de longo prazo.

O valor social da *Web* está nas novas possibilidades de comunicação humana, comércio e compartilhamento de conhecimentos. Um dos principais objetivos do W3C é tornar esses benefícios disponíveis para todas as pessoas, independente do *hardware* que utilizam, *software*, infraestrutura de rede, idioma, cultura, localização geográfica ou capacidade física e mental.

O número de diferentes tipos de dispositivos que podem acessar a *Web* cresce a cada dia. Desde telefones celulares, smartphones, PDAs, sistemas interativos de TV, sistemas de comandos de voz, quiosques e até mesmo alguns eletrodomésticos podem acessar a *Web*. A visão do W3C para a *Web* pressupõe a participação e o compartilhamento de conhecimentos para gerar confiança em uma escala global.

O escritório brasileiro do W3C é hospedado pelo Comitê Gestor da Internet no Brasil (CGI.br), cujos objetivos são coordenar e integrar todas as iniciativas de serviços Internet no país, promovendo a qualidade técnica, a inovação e a disseminação dos serviços ofertados. Para executar suas atividades, o CGI.br criou uma entidade civil, sem fins lucrativos, denominada Núcleo de Informação e Coordenação do Ponto BR (NIC.br).

Com base nesses princípios, o W3C Brasil desenvolveu o "Decálogo da *Web* Brasileira"[181], cujas diretrizes são: *Web* para todos; *Web* em todas as coisas; *Web* organizada em padrões; *Web* acessível; *Web* confiável; *Web* de múltiplos autores e leitores; *Web* a serviço da democracia; *Web* para o desenvolvimento social e econômico; *Web* que preserva sua memória e *Web* de todos.

O W3C Brasil, com base no "Decálogo da *Web* Brasileira", focou em três áreas de atuação no ano de 2011, que têm gerado diversos produtos em 2012: Plataforma para *Web* Aberta; Acessibilidade na *Web* e Dados Abertos. Com seis membros filiados (Caixa, iLearn, NIC.br, PUC-Rio, Senac-SP e SERPRO), o escritório do W3C Brasil também tem outros parceiros nacionais (Associação Brasileira de Entidades Estaduais de Tecnologia da Informação e Comunicação – ABEP, Controladoria Geral da União, Governo do Estado de São Paulo, Governo do Rio Grande do

[181] Decálogo da *Web* Brasileira. Disponível em: <http://www.w3c.br/decalogo/>.

Sul, Laboratório de Cultura Digital, Ministério do Planejamento, Perl Mongers, e Rede Nossa São Paulo) e internacionais (Agencia de Gobierno y la Sociedad de la Información de Uruguay – AGESIC, Ciudadanos Inteligentes de Chile, Comissão Econômica para América Latina e Caribe – CEPAL, UNESCO e IDRC do Canadá), conforme figura abaixo.

Fonte: Escritório Brasileiro do W3C.

Acessibilidade na *Web*

Acessibilidade na *Web* significa permitir e promover o acesso de pessoas com deficiências na *Web*. Segundo o Censo do IBGE de 2010, 24% da população brasileira (45.623.910 pessoas) tinha algum tipo de deficiência. Dessas deficiências, a maioria está relacionada a deficiência visual: são 35.791.488 pessoas com algum tipo de dificuldade para enxergar, incluindo pessoas cegas, que somam 528.624 pessoas.

Para a criação de páginas *Web* acessíveis existem diretrizes internacionais de acessibilidade criadas pelo W3C, são as WCAG (Web Content Accessibility Guidelines)[182] que orientam desenvolvedores para codificarem suas páginas de forma que não criem barreiras de acesso a pessoas com deficiência. Segundo

[182] Disponível em: <http://www.w3.org/TR/WCAG/>.

dados da pesquisa *Dimensões e características da Web brasileira: um estudo do domínio .gov.br*[183] de 2010, apenas 2% das páginas governamentais brasileiras eram acessíveis. No ano seguinte a mesma pesquisa registrou um aumento nesse número, que saltou para 5%. Ainda é um número baixo, mas um grande salto indicativo de que a acessibilidade na *Web* começa a ser levada em consideração nos projetos *Web* sob o domínio ".gov.br".

Desde a inauguração do escritório brasileiro do W3C, a instituição promove ações para fomentar e ampliar a discussão de acessibilidade na *Web* no Brasil. Até agosto de 2012 foram mais de 40 palestras no Brasil e no exterior disseminando os padrões para uma *Web* mais acessível.

Desde 2009, o W3C Brasil promove ações durante o Dia 3 de dezembro, proclamado pela ONU como o Dia Internacional da Pessoa com Deficiência. Todos os anos, nesse mesmo dia o Website do W3C Brasil sofre uma intervenção para lembrar as pessoas da importância da acessibilidade na *Web*.[184] São três tipo de páginas, três tipos de experiência de navegação: uma página toda escura, outra com o teclado bloqueado e outra com as fontes ampliadas. É uma iniciativa que mostra que é simples desenvolver uma página *Web* atendendo critérios de acessibilidade.

Em 2011 o Escritório Brasileiro do W3C lançou o Prêmio Nacional de Acessibilidade na *Web* – Todos@Web, para premiar pessoas e empresas que desenvolveram iniciativas relevantes a favor da acessibilidade na *Web*, *Websites* que sigam adequadamente os padrões e sejam acessíveis para pessoas com deficiência e tecnologias assistivas inovadoras para que pessoas com deficiência tenham autonomia no acesso a *Web*. Os vencedores da primeira edição do prêmio foram conhecidos em junho de 2012, em uma grande cerimônia que ocorreu no Memorial da Inclusão em São Paulo e contou com mais de 300 pessoas.[185]

Dados Abertos

Dados abertos é a disponibilização de informações representadas em formato aberto e acessível de tal modo que possam ser reutilizadas, misturadas com informações de outras fontes, gerando novos significados. Com mais especifici-

---

[183] Disponível em: <http://www.cgi.br/publicacoes/pesquisas/govbr/>.

[184] Disponível em: <http://w3c.br/3-dezembro/>.

[185] Disponível em: <http://premio.w3c.br/>.

dade, são dados em computadores em formato tal que podem ser acessados por outros computadores por meio da Internet para produzirem aplicações e informações a partir do tratamento e transformação dos dados originais, misturados ou não com outros dados de outros computadores.

O W3C globalmente tem produzido tecnologias e padrões que possibilitam a publicação e reutilização dos dados em formato aberto. Essas tecnologias e padrões, por estarem em formato aberto e licenças livres, podem ser utilizadas gratuitamente por qualquer pessoa.

No entanto, a produção, transformação, publicação e reutilização de dados abertos não são tarefas das mais triviais. Apesar de fáceis, exigem conhecimento técnico, atenção com processos e aspectos legais e infraestrutura tecnológica simples, mas que seja estável e escalável.

O W3C Brasil desenvolve uma série de atividades para fomentar a implementação consistente e permanente de dados abertos pelas organizações e o desenvolvimento de uma política pública consistente sobre o tema.

Em 2011, o W3C Brasil publicou manuais com o objetivo de atender diferentes públicos interessados no tema. O *Manual de Dados Abertos – Governo*[186], uma tradução com acréscimos locais do original *Open Data Manual*, da Open Knowledge Foundation. Foi o primeiro manual em português sobre o tema e tinha como alvo delinear os conceitos e as melhores práticas para os gestores públicos. O segundo manual, O *Manual de Dados Abertos – Desenvolvedores*[187], apresentou à comunidade de desenvolvimento *Web* como publicar e reutilizar dados em formato aberto.

Um projeto consistente de dados abertos pressupõe a participação de técnicos com conhecimento de padrões abertos para formatos de dados, e, se possível, vocabulários e ontologias. O W3C Brasil ofereceu dois cursos sobre *Como Publicar Dados Abertos*[188] e *Aspectos Básicos e Avançados de Engenharia de Ontologias* para técnicos do governo brasileiro com objetivo de apoiar o desenvolvimento da Infraestrutura Nacional de Dados Abertos (INDA), com coordenação no Ministério do Planejamento.

---

[186] Disponível em: <http://www.w3c.br/Cursos/CursoDadosAbertos>.

[187] Disponível em: <http://www.w3c.br/pub/Materiais/PublicacoesW3C/manual_dados_abertos_desenvolvedores_Web.pdf>.

[188] Disponível em: <http://www.w3c.br/cursos/dados-abertos/saopaulo-2010-06/>.

A quantidade de dados governamentais com potencial de serem publicados em formato aberto é imenso e as demandas por dados pelas organizações da sociedade civil são igualmente imensas. O ponto ótimo entre a oferta e a demanda é quando as ofertas e demandas coincidem. Para tanto, o W3C Brasil criou um Grupo de Trabalho de Dados Abertos que reúne diversos órgãos públicos que possuem dados de interesse público e organizações da sociedade civil que buscam dados governamentais para aprimorar as suas ações. Esse grupo obteve em 2011, por meio de consenso, uma matriz de prioridades que definem 10 áreas nas quais dados existentes são mais relevantes e possíveis de serem disponibilizados. A meta é conseguir no final de 2012 até 2 bancos de dados disponíveis em formato aberto.

Como resultados dessas ações, os governos começam a publicar seus dados em formato aberto. O Governo do Estado de São Paulo aumentou o número de base dados abertas disponíveis. A Câmara dos Deputados oferece uma API (Interface de Programação de Aplicativos) para acesso a dados. O Tribunal de Contas do Município do Estado do Ceará também está publicando dados orçamentários dos municípios cearenses.

Outro resultado das ações do W3C Brasil nesse tema é a repercussão internacional e o convite para participar de uma iniciativa latino-americana de fomento de dados abertos como política pública. O Projeto Open Data for Latin America (OD4D) teve início no segundo semestre de 2011 e promoveu um seminário no Rio de Janeiro, o primeiro na América Latina para diferentes países da região sobre o tema.

Um resultado particularmente especial para o W3C Brasil foi a sanção da Lei de Acesso à Informação pela presidente da República, Dilma Rousseff. Não somente pelo acesso à informação garantido como um direito, mas também pela inclusão de um artigo que exige que as informações sejam publicadas em sítios da Internet e estes possibilitem o acesso automatizado por sistemas externos em formatos abertos, estruturados e legíveis por máquina. Fruto de um trabalho articulado do W3C Brasil e muitas outras organizações que subsidiaram a elaboração do texto final, a nova lei abre uma enorme possibilidade de crescimento do uso de dados abertos a partir da entrada em vigor em 2012.

Plataforma para a *Web* Aberta

A Plataforma para a *Web* Aberta consiste em um conjunto de tecnologias desenvolvidas pelo World Wide Web Consortium, junto com outros parceiros, que foi definida em 2011 pelo CEO do W3C, Jeff Jaffe, como "uma plataforma para inovação, consolidação e eficiência" para a Internet.

Essa coleção de tecnologias é composta por código e especificações que são desenvolvidas dentro de *working groups* (grupos de trabalho) hospedados e promovidos pelo W3C. São mais de 500 indivíduos que participam desses grupos de trabalho e pertencem às organizações afiliadas ao consórcio. Além de mais de 100 profissionais trabalhando em tempo integral no desenvolvimento de uma *Web* para todos.

Juntamente com outras iniciativas do W3C, como Dados Abertos e o próprio Decálogo, a Plataforma para uma *Web* Aberta permite que a *Web* possa contar com interfaces acessíveis, interoperáveis, de conteúdo *linkado* e classificado de modo a facilitar o trabalho de busca, entregando para o usuário uma experiência mais completa de uso da *Web*.

O modo de funcionamento do consórcio está voltado para a produção de componentes de código aberto (*Open Source*) o que possibilita sua implementação sem custos ou taxas de licenciamento. Os focos principais da Plataforma para a *Web* Aberta são:

- Promover a *Web* Semântica;
- Facilitar o acesso *off-line*;
- Acesso através de diversos dispositivos;
- Promover a melhoria da conectividade para melhor comunicação;
- Melhorar a integração, a experiência e a performance de aplicativos e conteúdos *Web*.
- Oferecer efeitos e interações ricas acessíveis, através do CSS3;

Abaixo um pequeno panorama sobre algumas tecnologias que nos últimos dois anos foram recomendadas pelo W3C para a construção da *Web* Aberta. A aderência aos padrões recomendados é diretamente proporcional à qualidade de serviços prestados, visto que permite o uso da *Web* em seu potencial máximo.

- **HTML5:** é a quinta versão do HTML, que é a linguagem de marcação utilizada para que os navegadores possam interpretar conteúdos. O HTML5 tem como objetivo apresentar conteúdos multimídia de modo mais acessível e integrado, além de melhorar a consistência para melhor compreensão dos conteúdos por parte de máquinas.
- **CSS3**: é a versão mais nova das CSS, que existem para aplicar estilos às páginas em HTML. O CSS3 apresenta novas possibilidades para a *Web* porque permite efeitos para interações ricas, como animações e transições, por exemplo.
- **SVG**: é uma linguagem para descrever desenhos e gráficos de forma vetorial, ou seja: o SVG permite que máquinas leiam o conteúdo de uma imagem, diferente das imagens em formato JPEG ou PNG, por exemplo. Além disso, possibilita que uma imagem não perca qualidade ao ser ampliado. O SVG é o único formato vetorial aberto e foi criado pelo W3C em 1998.
- **WAI-ARIA**: (Web Acessibility Iniciative – Accessible RIch Internet Applications) é um conjunto de recomendações do W3C para acessibilidade em interações ricas;
- **MathML**: é uma recomendação utilizada para representar símbolos e fórmulas matemáticas. Foi criado pelo grupo de trabalho em matemática do W3C;
- **WebGL:** (Web Graphics Library) é uma API em Javascript (linguagem baseada em ECMAScript) que possibilita renderização para elementos 2D e 3D através do elemento canvas do HTML5.
- **Web Storage:** são recomendações e protocolos utilizados para armazenar dados no browser, de maneira similar aos cookies, porém sem o armazenamento de informações no Http request header. Isso significa melhor segurança e conformidade dos dados.
- **Indexed Database**: é um padrão recomendado para armazenamento de dados com entrada pelo navegador. Ele possibilita, por exemplo, que browsers diferentes tenham acesso à customizações únicas, como por exemplo bookmarks;

- **Web Sockets Protocol/API**: É um protocolo que permite suprir necessidades de atualização em tempo real, superando as limitações do protocolo HTTP. O protocolo WebSocket é um esforço para que aplicações ofereçam conectividade com zero de latência entre clientes e servidores *Web*.
- **Geolocation**: é uma recomendação que pretende fornecer a localização de qualquer objeto do mundo real para a *Web*.

Nos últimos dois anos o W3C Brasil vem promovendo a Plataforma para a *Web* Aberta entre a comunidade de desenvolvedores *Web*. Foram oferecidos cursos de HTML5[189] e de CSS3[190] que capacitaram diversos profissionais do mercado, particularmente aqueles ligados a instituições de treinamento, com o objetivo de replicar conhecimento. Para reforçar o aprendizado dos cursos, foi criada uma lista de discussão[191] sobre HTML5 que agrega não só ex-alunos dos cursos mas outros interessados no tema.

Mesmo antes da Plataforma para a *Web* Aberta ter se consolidado como um padrão oficial do W3C (muitos módulos do HTML5 e CSS3 ainda estão em fase de testes) ela tem se tornado um padrão de fato. No Brasil, observamos que grandes corporações já passaram a disponibilizar o seu conteúdo para HTML5 (por exemplo, Folha de S. Paulo e Globo.com), reconhecendo nessa plataforma o valor que ela oferece.

Concluindo, observamos que a *Web* brasileira vem aos poucos se organizando em padrões, cada vez mais adotando padrões abertos de acessibilidade e de interoperabilidade. No entanto, ela não está imune à disputa que é travada no mercado entre uma *Web* aberta e para todos e uma plataforma de *apps* (aplicativos) fechada, principalmente nos dispositivos móveis, que aprisiona seus usuários e coloca barreira à livre troca de conteúdos. As lojas e apps dos smartphones não podem ser referenciados (por exemplo, adicionados como favoritos ou linkados por e-*mail* ou Twitter) pois estão fora da *Web*.

É necessário ficar atento, cada vez mais. Como disse Tim Bernerts-Lee: "A *Web* é decisiva não só para a revolução digital, mas para a contínua prosperidade e liberdade individual. Como a democracia, a *Web* deve ser defendida e preservada".[192]

---

[189] Disponível em: <http://www.w3c.br/Cursos/CursoHTML5>

[190] Disponível em: <http://www.w3c.br/Cursos/CursoCSS3>

[191] Disponível em: <https://mail.nic.br/mailman/listinfo/w3c_html5>

[192] Artigo de Tim Berners-Lee para a Revista American Scientific Brasil. Disponível em: <http://www2.uol.com.br/sciam/reportagens/vida_longa_a_web.html>.

9

Debates relevantes em outros países

9.1 Estados Unidos da América

9.1.1 SOPA e PIPA

O SOPA (*Stop On-line Piracy Act*) e o PIPA (*Protect Intellectual Property Act*) são dois projetos de lei norte-americanos que buscam regulamentar o conteúdo disposto na Internet, com o objetivo de proteger direitos de propriedade intelectual e combater a pirataria *on-line*.

O SOPA foi apresentado pelo presidente do Comitê Judiciário da Câmara dos Deputados, Lamar Smith, Texas, em 26 de outubro de 2011. Seu objetivo é conferir ao governo americano maior capacidade de enfrentar as violações a direitos autorais que ocorrem no meio digital, além de evitar o compartilhamento de conteúdos protegidos por direitos autorais entre os usuários da Internet. Segundo o preâmbulo do projeto, ele busca "promover a prosperidade, a criatividade, o empreendedorismo e a inovação, combatendo o roubo da propriedade americana, e outros motivos".

Em linhas gerais, o projeto trata da transmissão *on-line* de obras protegidas por direitos autorais, conteúdo que viole leis criminais, do tráfico de bens ou serviços perigosos e da defesa dos direitos de propriedade intelectual. Além disso, confe-

re poderes ao procurador geral para proteger consumidores norte-americanos e impedir o apoio dos EUA a *sites* estrangeiros infringentes às leis vigentes. Também estabelece um sistema de prevenção contra o financiamento americano a *sites* dedicados ao roubo de propriedade norte-americana e confere imunidade a provedores de serviço para agir voluntariamente contra esses *sites* e contra *sites* que ponham em perigo a saúde pública.[193]

O PIPA também é chamado de *Preventing Real On-line Threats to Economic Creativity and Theft of Intellectual Property Act*, ou Lei de Prevenção a Ameaças Reais *On-line* à Criatividade Econômica e ao Roubo de Propriedade Intelectual. Foi proposto pelo senador Patrick Leahy no dia 12 de maio de 2011, sendo uma reformulação do Projeto de Lei de Combate à Violação e Falsificação *On-line* (Coica), rejeitado pelo Parlamento norte-americano em 2010. De maneira semelhante ao SOPA, o *Protect IP Act* objetiva "prevenir ameaças *on-line* à criatividade econômica e o roubo de propriedade intelectual, e outros motivos".[194]

Este projeto objetiva reforçar a execução judicial contra *sites* operados e registrados fora dos Estados Unidos, além de eliminar os incentivos financeiros de violação à propriedade intelectual no meio digital e disciplinar ações voluntárias contra *sites* que violem direitos de propriedade intelectual de acordo com as leis norte-americanas.[195]

Embora ambos tenham o propósito de evitar o *download* ilegal e outras formas de pirataria, estabelecendo assim sistemas de remoção de *sites* considerados pelo Departamento de Justiça como "dedicados a atividades infringentes", eles possuem diferenças substanciais quanto ao seu conteúdo. Enquanto o SOPA afetará qualquer *site* que cometer ou propiciar violações a direitos autorais, o PIPA trata apenas daqueles cuja atividade é em si violadora desses direitos.[196] De maneira exemplificativa, o primeiro poderá atingir *sites* como *blogs*, redes sociais, provedores de vídeo e de *e-mail*, *sites* de busca, etc.; já o segundo atingirá apenas *sites* de compartilhamento de arquivos, na medida em que esses arquivos violem direitos autorais.

Os projetos também divergem quanto à forma. O SOPA determina que *sites* infringentes sejam retirados de qualquer ferramenta de busca, o que não é pre-

---

[193] Conceitos extraídos dos títulos do Projeto de Lei SOPA.

[194] Texto extraído do preâmbulo do Projeto de Lei PIPA.

[195] Conceitos extraídos dos títulos do Projeto de Lei PIPA.

[196] INTERNATIONAL BUSINESS TIMES. *SOPA and PIPA Bills: Differences Between the Two Internet Privacy Acts* Disponível em: <http://www.ibtimes.com/articles/283906/20120118/sopa-pipa-bills-differences-Internet-privacy-senate.htm>. Acesso em 14 de fevereiro de 2012.

visto pelo PIPA. Além disso, o PIPA demanda mais intervenção do Judiciário para que um *site* seja retirado do ar; porém, não apresenta nenhuma disposição que penalize o detentor de direitos autorais que, sabendo que não existe violação a esses direitos, mesmo assim ajuizar ação contra um *site* hipoteticamente infringente.[197] Diferentemente, o SOPA determina que, nesse caso, o detentor será responsável pelos danos e custos legais.

9.1.1.1 Críticas dos oponentes ao SOPA e ao PIPA

Muitas críticas a ambos os projetos foram feitas pela mídia, por instituições e pela sociedade civil no fim de 2011, na sua maioria de forma indiscriminada devido à grande semelhança entre os projetos. Nesse sentido, sobressai a atuação da EFF (*Eletronic Frontier Foundation*), instituição norte-americana que procura defender direitos no mundo digital, que se manifestou continuamente em seu *site*, através de diversos artigos analisando os projetos e suas repercussões, e também a atuação do Google, que organizou uma petição *on-line*[198] contra os projetos.

Basicamente todas as críticas foram pautadas em dois pilares: possíveis ameaças (I) aos direitos autorais e (II) à capacidade inovadora conferida à sociedade pela Internet livre. Também foi quase unânime entre os opositores aos projetos, a opinião de que eles acarretarão censura na *web* a nível mundial, uma vez que conferem ao governo dos EUA o direito de retirar conteúdo da rede, abrigado em qualquer território nacional, justificando-se com termos vagos, além de conceder legitimidade a provedores de Internet para bloquear *sites* inteiros arbitrariamente, sem a necessidade de prévia decisão judicial.

Outros pontos tratados pelos projetos ganharam destaque. O primeiro diz respeito à questão da responsabilidade civil por conteúdo disponibilizado na *web*. Segundo os projetos, os *sites* em geral (de jornais, revistas, portais de vídeo e música e redes sociais) seriam corresponsáveis pela postagem e replicação de *links* considerados nocivos. Muitos *sites* possuem espaço para comentários, como *blogs*, *sites* de notícias, etc. e, mesmo que os *links* sejam introduzidos nesse espaço, o *site* responderá civil e penalmente. Os projetos adicionam um fator agravante à característica participativa de *sites* que existem devido à atuação dos usuários, de forma

---

[197] SOCIAL MEDIA COLLECTIVE RESEARCH BLOG. *What's the difference between SOPA and PIPA?* Disponível em: <http://socialmediacollective.org/2012/01/17/whats-the-difference-between-sopa-and-pipa/>. Acesso em 14 de fevereiro de 2012.

[198] Disponível em <https://www.google.com/landing/takeaction/>. Acesso em 17 de fevereiro de 2012.

que seu conteúdo não passa por nenhum processo de moderação, como redes sociais, *microblogs* ou portais de vídeo – esses, portanto, teriam grandes chances de saírem do ar, caso não fizessem um controle do conteúdo em si disposto. O controle de conteúdo não só descaracteriza a existência desses *sites*, como também lhes impõem uma aplicação ineficiente de custos em monitoramento.

Observa-se que os provedores de Internet e as empresas responsáveis por *sites*, para não serem submetidos a um litígio no Judiciário norte-americano contra o governo, são praticamente obrigados a monitorar seus usuários. Essa seria uma nova atividade a ser desenvolvida na empresa, acarretando a elas novos custos, crescentes na medida dos riscos sofridos pelo *site*. Convenientemente, os projetos outorgam imunidade aos provedores de serviço para bloquear qualquer usuário ou *sites* voluntariamente, sem a necessidade de uma ordem judicial prévia, caso acreditem que esteja violando ou promovendo violações aos direitos autorais. O único requisito para tanto é que atuem de **boa-fé**. Dessa forma, corporações poderiam criar uma *blacklist* arbitrária, sem legitimações legais concretas para tais atos. Essa é uma disposição criticada por abrir brechas para o abuso de poder, além de recair diretamente sobre pessoas que não tenham violado direitos de nenhuma maneira.

O fato de a lei afetar pessoas não infringentes é uma das maiores preocupações da mídia. Os projetos determinam que o procurador geral concentrará uma série de amplos poderes e funções – o exemplo mais extremo seria a possibilidade de determinar que o Judiciário confira uma ordem de retirada completa do *site* do ar, em vez de retirar apenas a página, o texto ou o *link* infringente. Esse caso restringe tanto o direito de liberdade de expressão de pessoas que não estão violando nenhum direito de propriedade intelectual, quanto o direito dos usuários de terem acesso à informação constante naquele *site*. Os próprios autores do conteúdo ali depositado estariam impedidos de acessar suas criações. Alex Mcgillivray, conselheiro geral do Twitter, manifestou-se sobre esse assunto no *blog* Bricoleur, em *post* denominado "*Overbroad Censorship & Users*".[199]

Outro segmento social prejudicado seria a comunidade internacional de *software* aberto que, segundo a EFF[200], se utiliza de *virtual private networks*, *proxys* ou *softwares* de privacidade e anonimação (*software* de segurança na Internet)

---

[199] Disponível em <http://www.bricoleur.org/2011/12/overbroad-censorship-users.html>. Acesso em 17 de fevereiro de 2012.

[200] Disponível em: <https://www.eff.org/deeplinks/2012/01/how-pipa-and-sopa-violate-white-house-principles-supporting-free-speech> e <https://www.eff.org/deeplinks/2011/11/hollywood-new-war-on-software-freedom-and-Internet-innovation>. Acesso em 17 de fevereiro de 2012.

para lutar contra governos autoritários que censuram diretamente a Internet. A Internet tem servido cada vez mais como viabilizadora de mobilizações sociais, devido à grande facilidade de compartilhamento de informações e de comunicação. Ativistas digitais são conhecidos por utilizar-se de ferramentas *on-line* em sua luta a favor da democracia em países como China, Irã, Tunísia, etc. Tais ferramentas permitem que burlem as tentativas dos governos de bloquear conteúdo na Internet para diminuir as manifestações contrárias às suas políticas. De acordo com o SOPA e o PIPA, os *sites* que indicassem como burlar as regras por eles impostas se tornariam um alvo do governo norte-americano.

Como visto, a transmissão não autorizada de conteúdo protegido por direitos autorais seria cassada tanto pelo procurador geral, que seria legitimado a atuar por meio do Judiciário, quanto pelos próprios provedores de serviço, que incorreriam em riscos devido à alta responsabilidade a eles imposta. Por exemplo, quem postar um vídeo de si mesmo cantando qualquer música protegida por direitos autorais poderia ser preso por até cinco anos; um vídeo de si mesmo jogando um *videogame*, como forma de demonstrar o desenvolvimento pessoal naquele jogo, poderia, da mesma forma, ser excluído da rede. Nesse caso, a desenvolvedora do jogo deveria solicitar o banimento do vídeo. O *site* hospedeiro do vídeo seria notificado e, em caso de não cumprimento e consequente reincidência no pedido, poderia ter todo o seu conteúdo bloqueado até que o fato fosse resolvido.

Sites considerados infringentes, além de terem seu conteúdo repreendido, estariam sujeitos à exclusão do seu domínio dos *sites* de busca, caso não acatassem às ordens judiciais em até cinco dias após o recebimento da notificação. Além disso, estariam impedidos de obter qualquer financiamento ou remuneração *on-line*, prejudicando, assim, os *service payment providers*, que, de acordo com os projetos, adquirem a responsabilidade de prevenir, proibir ou suspender seus serviços de transações de pagamento a *sites* infringentes, localizados nos EUA ou sob sua jurisdição. Serviços de anúncios na Internet são igualmente prejudicados, na medida em que não poderão fazer anúncios em *sites* considerados infringentes ou sobre tais *sites*.

Existe, ainda, uma intensa preocupação com o direito à privacidade, uma vez que os IPs de cidadãos norte-americanos poderiam ser filtrados para que fosse encontrado conteúdo ofensivo. Além disso, provedores de *e-mail* poderiam bloquear *links* localizados dentro da própria caixa postal de um indivíduo, no corpo de um *e-mail*.

Por fim, o projeto não afeta somente *sites* localizados nos EUA – possui uma seção apenas sobre *sites* estrangeiros infringentes, que ganham esse status se

"comete(m) ou facilita(m) o cometimento" de violações de artigos específicos de leis americanas, que possuem relação com direitos autorais e de propriedade intelectual. Os próprios provedores terão até cinco dias para tomar medidas técnicas com o fim de impedir o acesso dos usuários localizados nos EUA ao *site* considerado infringente, caso recebam ordem judicial assim determinando. Os processos judiciais são iniciados pelo procurador geral, que decidirá se aquele *site* está infringindo direitos autorais e de propriedade intelectual.

As notícias apontam como pessoas beneficiadas desses projetos aquelas que são constantes alvos da pirataria, como as indústrias produtoras de conteúdo (cinematográfica e fonográfica), as emissoras de televisão e os desenvolvedores de jogos.

9.1.1.2 O *Blackout*

As oposições contra os projetos de lei americanos antipirataria SOPA e PIPA tiveram enorme repercussão, principalmente no ambiente digital, resultando no maior protesto *on-line* da história. No dia 18 de janeiro de 2012, foi organizado um *blackout* na rede, isto é, *sites* sairiam voluntariamente do ar, retirando seu conteúdo ou parcela desse, ou vinculando mensagens de oposição em suas páginas iniciais. O movimento ganhou maior atenção quando gigantes da rede se manifestaram a favor do protesto, como Wikipedia, Google, Reddit, Wordpress, dentre outros, e resultou na não votação dos projetos, que estava prestes a acontecer.

Segundo dados do *site Fight for the Future*, um dos maiores grupos de ativistas a organizar o SOPA *Strike*, mais de 115 mil *sites* participaram do *blackout* e foram enviados por volta de 4 milhões de *e-mails* ao Parlamento americano.[201] Além disso, os representantes americanos eleitos receberam por volta de 8 milhões de ligações da sociedade para contestar os projetos de lei – uma outra forma de manifestação, desvinculada do ambiente digital.

A Google apresentou papel determinante na luta contra o SOPA e o PIPA. Junto com as empresas AOL, Ebay, Facebook, Twitter, Firefox, Linkedin e Zynga, enviou uma carta aberta em objeção aos projetos ressaltando os riscos que trazem para a inovação e a criação de novos empregos. Outras cartas também foram enviadas por 17 fundadores de empresas de Internet, 39 organizações de advocacia e de interesse público, 41 organizações de direitos humanos, 110 professores de

[201] Disponível em: <http://www.sopastrike.com/numbers/>. Acesso em 23 de fevereiro de 2012.

direito, 204 empreendedores. Mais de 113 mil pessoas assinaram uma petição enviada à Casa Branca, negando apoio a legislações que violem a liberdade de expressão, aumente o risco de segurança na rede e comprometa as características da dinamicidade e inovação da Internet global. [202]

Cabe ressaltar que as manifestações e participações no *blackout* não ocorreram apenas em território americano. Em todo o mundo pessoas se viram ameaçadas pelos projetos de lei que, embora atuem apenas em jurisdição norte-americana, afetam o acesso global à Internet.[203] Um *site* considerado suspeito de infração às leis antipirataria poderia ser bloqueado sem a necessidade de uma ordem judicial. Considerando que grande parte da infraestrutura da Internet está localizada em território americano, ou hospedada em plataformas americanas sem que exista discriminação para acesso, pessoas ao redor de todo o mundo seriam prejudicadas, uma vez que acessam diariamente tais *sites* com finalidades legítimas (isto é, não relacionadas com a prática de pirataria). Por conta desse fato, muitos opositores afirmaram que o SOPA e o PIPA estariam ameaçando características fundamentais da rede: a universalidade e a neutralidade.

No Brasil, ajudaram a organizar o *blackout* (I) o movimento Mega Não!, que busca combater o vigilantismo, as ameaças à liberdade na Internet e à neutralidade da rede, (II) o Coletivo Trezentos, um blog que busca materializar a característica participativa da Internet por ter seu conteúdo escrito por diversos autores, e (III) o *software* Livre Brasil, uma iniciativa não governamental que incentiva a produção sustentável através dos benefícios das novas tecnologias, como a alta capacidade de compartilhamento de conteúdo e informação. [204]

Participaram do *blackout*, dentre outros, o Instituto Brasileiro de Defesa do Consumidor (Idec) e todos os *sites* vinculados ao Centro de Tecnologia e Sociedade da escola de Direito da Fundação Getulio Vargas (CTS-FGV). O Idec veiculou em sua página inicial uma mensagem afirmando que "a liberdade e os direitos dos

---

[202] Dados retirados do infográfico da Google, disponível em: <https://www.google.com/landing/takeaction/>. Acesso em 23 de fevereiro de 2012.

[203] O Twitter, através de afirmação do CEO do microblog, Dick Costolo, reconheceu que os projetos podem afetar mais do que os nacionais americanos ao afirmar que "é muita irresponsabilidade nossa parar um serviço global por conta de uma lei nacional". Disponível em: <http://www.portalmariana.org/internet/os-grandes-sites-da-internet-protestam-contra-os-projetos-de-leis-antipirataria-sopa-e-pipa/>. Acesso em 23 de fevereiro de 2012.

[204] Disponível em: <http://meganao.wordpress.com/o-mega-nao/o-que-combatemos/>. Acesso em 23 de fevereiro de 2012.

usuários de Internet no mundo todo estão ameaçados". Assim como o CTS-FGV, o instituto manifestou-se antagonicamente ao projeto de lei brasileiro semelhante ao SOPA e ao PIPA, chamado "Lei Azeredo", que visa a criminalização de condutas praticadas através do ambiente digital, incluindo-se nesse rol a pirataria. Assim, organizou, em 2011, uma campanha intitulada "Consumidores contra o PL Azeredo", que reuniu mais de 16 mil assinaturas.[205]

Já o CTS-FGV produziu, em conjunto com o Ministério da Justiça e por meio de um processo *on-line* amplamente colaborativo, o Marco Civil da Internet[206], projeto de lei que está atualmente em tramitação no Congresso Nacional. De acordo com Carlos Affonso de Souza, vice-coordenador do CTS-FGV, o Marco Civil da Internet é considerado um projeto de lei anti-SOPA, uma vez que, em vez de criminalizar condutas, reafirma princípios que devem permear a Internet e protege direitos fundamentais no ambiente digital.[207] "O CTS defende que a tutela dos direitos intelectuais não deve ser exercida em detrimento de outros direitos fundamentais, como a privacidade, a liberdade de expressão, e principalmente o acesso ao conhecimento e à informação".[208]

Algumas figuras importantes no cenário da Internet também manifestaram oposição ao SOPA e ao PIPA. Como exemplo, pode-se citar a afirmação de um dos fundadores da *worldwide web* (www), Tim Berners-Lee, de que os projetos desrespeitam direitos humanos: "Se você é um americano, então deveria ligar para alguém ou enviar um *e-mail* para protestar contra essas leis (de censura), porque elas não foram reunidas para respeitar direitos humanos como é apropriado em um país democrático"[209]. Já Vinton Cerf, um dos fundadores da Internet, enviou uma carta de contestação ao autor do SOPA, Lamar Smith, e aos membros do *House Judiciary Committee*, na qual afirmou que "o bloqueio de *sites* ou os meca-

---

[205] Mais informações no *site* <http://www.oficinadanet.com.br/noticias_web/4815/no-brasil-idec-tambem-se-manifesta-contra-a-lei-antipirataria>. Acesso em 23 de fevereiro de 2012.

[206] O texto legal do Marco Civil da Internet resultou de um processo de construção colaborativo, na medida em que foi organizado por meio da plataforma *on-line* Cultura Digital (<http://culturadigital.br/marcocivil/>) e reuniu comentários de todos os setores da sociedade, de forma não moderada e voluntária. Para saber mais sobre o projeto, acesse <http://www.nupef.org.br/sites/default/files/poliTICS_n%C2%BA7_1.pdf>. Acesso em 23 de fevereiro de 2012.

[207] Tal posicionamento pode ser encontrado nas reportagens: <http://www.info4.com.br/gomateria.asp?cod=600426&nome=1432&cliente=1432> e <http://oglobo.globo.com/tecnologia/artigo-discussao-da-sopa-ensaio-para-que-vira-no-futuro-3703202>. Acesso em 23 de fevereiro de 2012.

[208] Disponível em: <http://direitorio.fgv.br/sopablackout>. Acesso em 23 de fevereiro de 2012.

[209] Disponível em: < http://articles.businessinsider.com/2012-01-20/tech/30645823_1_human-rights-tim-berners-lee-sopa>. Acesso em 23 de fevereiro de 2012.

nismos de redirecionamento não são susceptíveis de fazer uma diferença significativa na disponibilidade de material ilícito e de falsificações *on-line*".[210]

Os protestos foram ainda reforçados pelas declarações do governo de Barack Obama, se posicionando contras as proposições, em resposta oficial a duas petições que pediam o veto aos projetos de lei. O comunicado, divulgado pelo *blog* da Casa Branca, sustentou que a importante tarefa de se proteger a propriedade intelectual *on-line* não pode ameaçar a abertura e o aspecto inovador da Internet.[211]

9.1.2 ACTA

9.1.2.1 Breve histórico

O *Anti-Counterfeiting Trade Agreement* (ACTA) ou Acordo Comercial Anticontrafação[212] é um tratado multinacional em fase de negociação que busca estabelecer padrões internacionais de tratamento aos direitos de propriedade intelectual e facilitar o combate às violações a nível global, através da cooperação internacional. Desenvolvido primeiramente pelos EUA e pelo Japão em 2006, desde então conquistou o apoio de muitos países ao redor do mundo, os quais participam dos encontros de negociação do texto do tratado e o assinaram em 2011.

No preâmbulo do tratado é possível encontrar as justificativas para a criação do ACTA. Nesse sentido, afirma que a proteção aos direitos de propriedade intelectual é essencial para a garantia do desenvolvimento econômico sustentável. Busca proteger, assim, o comércio legítimo, os titulares de direitos e as empresas legítimas, bem como combater o crime organizado.

O tratado prevê que cada país signatário possua mecanismos de solução judicial de litígios relativos a infrações a direitos de propriedade intelectual. Os mecanismos a serem utilizados são, dentro dos procedimentos judiciais de natureza cível, injunções, indenização do infrator ao titular de direitos, bem como o ressar-

---

[210] Disponível em: <http://www.examiner.com/internet-in-national/internet-founding-father-vinton-cerf-opposes-sopa>. Acesso em 24 de fevereiro de 2012.

[211] Disponível em: <http://www.whitehouse.gov/blog/2012/01/13/obama-administration-responds-we-people-petitions-sopa-and-online-piracy>. Acesso em 24 de fevereiro de 2012.

[212] A versão em português está disponível neste *link*: <http://register.consilium.europa.eu/pdf/pt/11/st12/st12196.pt11.pdf>. Acesso em 27 de fevereiro de 2012.

cimento dos lucros obtidos com a comercialização do material sem autorização e retirada de circulação ou destruição de materiais utilizados para a fabricação do material infrator. Também podem as autoridades judiciais ordenar a adoção de medidas provisórias com finalidade preventiva de infração ou de preservação de provas sobre a infração.

No que se refere a medidas que podem ser tomadas nas fronteiras, o tratado exclui de condenação pequenas quantidades de mercadoria não comercial transportada em bagagem pessoal, sem definir o termo pequenas quantidades.

As execuções de natureza penal só afetam atos infringentes que ocorram em escala comercial (que acarretem em benefícios econômicos para o infrator). Elas incluem responsabilização penal de sociedade de pessoas e indivíduos isolados, concedida a critério do país signatário, penas de prisão, sansões pecuniárias elevadas o bastante para que tenham caráter preventivo, apreensão, confisco e destruição de mercadoria.

O ACTA possui um capítulo específico sobre aplicação dos direitos de propriedade intelectual no ambiente digital. Afirmando que as partes se comprometem a combater violações a direitos autorais e direitos conexos em ambiente digital, o texto ressalva que tais medidas devem ser tomadas sem ferir ou ofender princípios fundamentais como a liberdade de expressão, a privacidade e o devido processo legal, além de não impedir os meios legítimos de comércio eletrônico e concorrência. Para tal, utiliza o termo **proteção jurídica adequada** e **recursos jurídicos eficazes**, sem especificar o que significam, apenas sugerindo minimamente como alcançá-los.

Existe, ainda, um artigo sobre a sensibilização do público. Assim, cada Estado signatário teria o dever de "promove(r) a adopção de medidas para sensibilizar a opinião pública no que se refere à importância do respeito dos direitos de propriedade intelectual e aos efeitos negativos do desrespeito desses mesmos direitos".[213]

9.1.2.2 Críticas dos opositores

Inicialmente, as negociações do ACTA eram secretas e apenas participavam países desenvolvidos.[214] A ausência de informações mais detalhadas sobre o que esta-

[213] Texto original em inglês – *Article 31: Public Awareness*: Each Party shall, as appropriate, promote the adoption of measures to enhance public awareness of the importance of respecting intellectual property rights and the detrimental effects of intellectual property rights infringement". Disponivel em <http://trade.ec.europa.eu/doclib/docs/2011/may/tradoc_147937.pdf>. Acesso em 22 de novembro de 2012.

[214] André de Mello e Souza, em reportagem publicava no Valor Econômico e transmitida pelo *blog* do

va sendo discutido e a consciência de que as deliberações sobre os direitos de propriedade intelectual afetariam não só os participantes das negociações, como também outros países não envolvidos e, inclusive, a própria sociedade dos países participantes fez com que um movimento forte de críticas fosse iniciado. A EFF (*Eletronic Frontier Foundation*) chegou a afirmar que a sociedade civil e os países em desenvolvimento estavam sendo excluídos das negociações intencionalmente.[215]

A população apenas tomou conhecimento do que estava sendo debatido através de documentos que vazaram ao longo dos anos, como o *Discussion Paper on a Possible Anti-counterfeiting Trade Agreement* ou relatórios de negociações ocorridas. Em maio de 2011, ocorreu a publicação oficial do texto do tratado, nas línguas inglês, francês e espanhol. Muitas das maiores preocupações relativas às versões anteriores do ACTA foram retiradas do texto oficial, o que demonstra que as críticas fizeram efeito nas negociações.[216] Em outubro de 2011, assinaram o tratado, além de EUA e Japão, Canadá, Austrália, Nova Zelândia, Singapura, Marrocos e Coreia do Sul.

Quanto ao conteúdo do tratado, os opositores afirmam que não abrangerá apenas produtos piratas na sua forma física, como CDs e remédios. O escopo atinge inclusive os intermediários de Internet, como os provedores de serviço de Internet, uma vez que o ACTA, da mesma forma que o SOPA e o PIPA, possibilita aos países signatários responsabilizar esses atores pelas ações de terceiros na rede. Assim, seriam obrigados a controlar a Internet e os usuários, o que gera preocupações grandes em relação aos direitos fundamentais, como privacidade e liberdade de expressão, além do *fair use* de direitos autorais. Segundo essa mesma linha de pensamento, também seriam limitados pelo ACTA a criatividade e inovação derivadas da característica colaborativa da rede.

As críticas também abarcam o processo de construção do texto do tratado, considerando-o antidemocrático, uma vez que careceu de transparência e não reconheceu a opinião de grupos da sociedade civil, do público em geral, de

---

projeto A2K: "a falta de transparência que caracteriza as negociações tem por finalidade evitar a oposição da comunidade internacional e contradiz a tendência recente dos fóruns multilaterais de permitir a observação e intervenção de organizações não governamentais e de divulgar os textos preliminares dos acordos na Internet". Disponível em: <http://www.a2kbrasil.org.br/wordpress/lang/pt-br/2010/09/o-acta-e-os-direitos-de-propriedade-intelectual/>. Acesso em 29 de fevereiro de 2012.

[215] Disponível em: <https://www.eff.org/issues/acta>. Acesso em 29 de fevereiro de 2012.

[216] Disponível em: <https://www.eff.org/deeplinks/2011/10/acta-signed-8-members-are-we-doomed-yet>. Acesso em 29 de fevereiro de 2012.

instituições internacionais, como a Organização Mundial do Comércio (OMC) e a Organização Mundial de Propriedade Intelectual (OMPI) e países em desenvolvimento. Como visto, nenhum desses atores teve acesso ao conteúdo tratado nas negociações até a divulgação do texto oficial em 2011, a não ser por vazamentos de informações das quais nem sempre se conhecia a fonte.

Por outro lado, um comitê consultivo de grandes corporações multinacionais americanas (membros da indústria farmacêutica e de produção cultural) foi consultado na fase de produção do rascunho e obteve, consequentemente, acesso a tal conteúdo. Além disso, as empresas Google, eBay, Intel, Dell, News Corporation, Sony Pictures, Time Warner e Verizon receberam uma versão do rascunho do tratado sob um acordo de confidencialidade. [217] Segundo o movimento brasileiro Mega Não!, "lobistas das grandes empresas de música, filmes, *software*, jogos de vídeo, bens de luxo e farmácia tiveram acesso a documentos preparatórios do ACTA e puderam influenciar as negociações".[218]

9.2 Espanha

Desde 2001, a Europa tenta adequar suas regras comuns à economia digital e ao mercado comunitário, com a Diretiva 2001/29 do Parlamento e do Conselho Europeu. A Diretiva trata da harmonização de certos aspectos do direito de autor e dos direitos conexos na Sociedade da Informação e demonstra, já nos seus considerandos que as novas tecnologias da informação gerou uma resposta repressiva por grande parte dos países:

"Qualquer harmonização do direito de autor e direitos conexos deve basear-se num elevado nível de proteção, uma vez que tais direitos são fundamentais para a criação intelectual. A sua proteção contribui para a manutenção e o desenvolvimento da atividade criativa, no interesse dos autores, dos intérpretes ou executantes, dos produtores, dos consumidores, da cultura, da indústria e do público em geral. A propriedade intelectual é, pois, reconhecida como parte integrante da propriedade".[219]

---

[217] Disponível em: <http://en.wikipedia.org/wiki/Anti-Counterfeiting_Trade_Agreement>. Acesso em 24 de fevereiro de 2012.

[218] Disponível em: <http://xocensura.wordpress.com/2008/09/22/o-silencio-sobre-o-acta/>. Acesso em 24 de fevereiro de 2012.

[219] A íntegra da Diretiva 2001/29 CE pode ser encontrada no seguinte *link*: <https://ciist.ist.utl.pt/docs_da/

A própria lei francesa que ficou conhecida como Lei Hadopi é fruto da transposição da Diretiva 2001/29 CE e implementa a regra dos "*three strikes and you're out*", a qual determina que, diante da reincidência do usuário que baixar obras protegidas sem autorização, sua conexão à Internet seria interrompida.

Em 2011, no entanto, a Espanha se juntou à França no grupo de países que adotam medidas mais fortes para a proteção da criação intelectual na Internet. As medidas, que foram introduzidas através da Lei de Economia Sustentável (LES), previam a possibilidade de bloqueio de páginas na Internet que facilitassem o download sem autorização de arquivos com conteúdo protegido por direitos autorais. Quando as medidas foram apresentadas em 2009, revelações do *Wikileaks* demonstraram que pressões do governo americano ao governo espanhol foram o principal motivo para que esse editasse uma medida contrária a *downloads*.

A Lei da Economia Sustentável (SEA) espanhola é fruto de uma iniciativa legal aprovada pelo governo espanhol, em 2009. Seu principal objetivo é modernizar a economia espanhola nos campos de finanças, negócios e meio ambiente, de forma a tentar solucionar a crise econômica que assola o país nos últimos anos. A versão original da SEA tem sido chamada de Lei Sinde – recebeu esse nome em virtude do Ministro da Cultura espanhol, Angeles Gonzales-Sinde, que apresentou a lei em resposta à demanda da coalizão de criadores e indústria de conteúdos, um grupo de pressão formado pelas sociedades de gestão de direitos e as sociedades que defendem os interesses das grandes companhias.

A função da Lei Sinde é legitimar o fechamento de *websites* que abriguem *links* para *download* de conteúdo protegido por direitos autorais. Desde o início, a Lei Sinde levantou diversas preocupações quanto à possibilidade de violação ao devido processo legal, ao direito à privacidade e à liberdade de expressão.

De acordo com documentos revelados pelo *Wikileaks* e divulgados pelo jornal espanhol *El País*, o governo norte-americano teve um papel crucial nas iniciativas de endurecimento da lei de direitos autorais da Espanha. Na referida reportagem de 2008, o periódico *El País*[220] revelou que o governo norte-americano ameaçou colocar a Espanha em sua lista anual de inimigos da propriedade in-

directiva_2001-29-CE.pdf>. Acesso em 20 de julho de 2012.

[220] Disponível em: <http://www.elpais.com/articulo/espana/EE/UU/ejecuto/plan/conseguir/ley/antidescargas/elpepuesp/20101203elpepunac_52/Tes>. Acesso em 20 de julho de 2012.

telectual, elaborada pela Câmara de Comércio, conhecida como "*Special* 301", a menos que o governo espanhol adotasse políticas para a pirataria na Internet.

O procedimento descrito pela lei para fechar *sites* da Internet se inicia com uma denúncia pelo titular de direitos autorais à Comissão de Propriedade Intelectual (órgão administrativo do Ministério da Cultura). Ao receber a denúncia e de forma a obter dados com a identidade do proprietário do nome de domínio, número de usuários do *site* e outros dados sujeitos a confidencialidade, a Comissão deve solicitá-los a um juiz. A presença da intervenção do Poder Judiciário desde o início do procedimento é tida como uma inserção de equidade ao processo. Porém, este não foi o entendimento quando a lei foi vetada em 2009.

Talvez pela divulgação dos documentos pelo *Wikileaks*, que revelaram a arquitetura diplomática dos Estados Unidos para influenciar na agenda jurídico-cultural espanhola, num primeiro momento a Lei Sinde foi rejeitada pelo Congresso Espanhol, por apoio de quase todos os partidos com representação parlamentar – à exceção de apenas um, o Partido Socialista Operário Espanhol (PSOE), como revela a citada reportagem do jornal *El País*:[221]

"*Para el PP, la disposición intentaba 'maquillar' con un procedimiento judicial rápido el que un órgano administrativo como la Comisión de Propiedad Intelectual, dependiente del Ministerio de Cultura, pudiera cerrar páginas webs. 'En la práctica, sería posible cerrar webs sin la debida garantía judicial, lo que abriría la puerta a que desde el poder político se vulnerasen derechos fundamentales como el de la libertad de expresión', según José María Lasalle. Marta Gastón, ponente del PSOE, le refutó que solo 'la justicia puede decidir el cierre de una web', y aseguró que no se puede 'desproteger a un sector que da empleo a 800.000 personas y representa el 4% del PIB'. Recordó que la subcomisión de Cultura acordó por mayoría dar unas garantías mínimas de protección a la propiedad intelectual, y afirmó: 'Si protegemos más a los ladrillos que las ideas, estaremos condenando a nuestros jóvenes a seguir fabricando ladrillos.'*" (grifo nosso)

Além da liberdade de expressão, outro direito fundamental atingido diretamente pelas disposições da Lei Sinde é a proteção à vida privada, uma vez que permite que os indivíduos que se julgam vítimas de alguma violação aos seus direitos de autor acessem dados pessoais de usuários. Precedente da Corte de Justiça da

[221] Disponível em: <http://cultura.elpais.com/cultura/2010/12/21/actualidad/1292886001_850215.html>. Acesso em 20 de julho de 2012.

União Europeia envolvendo a própria Espanha já rechaçou que provedores de acesso à Internet assumam postura em defesa dos titulares de direito autoral que ameacem a vida privada. Nesse sentido, o acórdão *Promusicae v. Telefónica* determinou que a exigência pelos titulares de direitos de propriedade intelectual do acesso aos dados de IP de indivíduos suspeitos de violação de direitos autorais é contrária às normas fundamentais da União Europeia..

9.3 Suíça

Em sentido contrário ao ocorrido na Espanha (Tópico 9.2), a Suíça decidiu não modificar sua legislação interna de propriedade intelectual no meio digital, por julgar que as normas existentes em seu ordenamento jurídico eram suficientes para tratar da realidade digital.

O Conselho Federal da Suíça foi chamado a se posicionar sobre o tema e preparou um relatório que foi divulgado no início de dezembro de 2011. O estudo analisou a possibilidade de constrição legislativa dos *downloads* ilegais e as medidas existentes no cenário internacional que tentam solucionar o problema. O governo suíço concluiu que uma nova lei ou reformas legislativas sobre a questão não são essenciais, ou mesmo necessárias, no momento. Seria preciso, ao contrário, acompanhar as evoluções tecnológicas e o debate sobre o tema ao nível internacional, a fim de reavaliar periodicamente a situação e identificar as necessidades de adaptação do direito autoral.

Para elaboração do relatório, o Conselho Federal analisou diversos estudos internacionais sobre *download* e compartilhamento de música, filmes e jogos eletrônicos. O estudo "*Ups and Downs: The Economic and cultural effects of file sharing on music, film and games*",[222] encomendado pelo governo da Holanda em 2009, foi usado como parâmetro pelo governo suíço para acessar os dados sobre pirataria. O uso crescente de *downloads* e o compartilhamento de bens culturais não diminuem a intenção das pessoas em adquirir outros bens culturais, como bilhetes de cinema, teatro e shows. E mesmo aqueles que adquirem os bens por *download* não deixam de comprá-los pelas vias tradicionais, segundo o relatório do governo suíço.

---

[222] Disponível em: <http://www.tno.nl/content.cfm?context=thema&content=inno_publicatie&laag1=897&laag2=918&item_id=473&Taal=2>. Acesso em 20 de julho de 2012.

Foram apontadas três abordagens existentes no cenário internacional para lidar com esse dilema. Cada uma foi rejeitada, justificadamente, conforme abaixo resumido:

9.3.1 Resposta graduada ou "three strikes and you're out" (modelo francês – Hadopi)

Os dados revelados pela autarquia francesa Hadopi, que tem por objetivo impedir a violação de direitos autorais na Internet, apontam uma queda no número de *downloads* e compartilhamento ilegal de arquivos na França em 2011. Mesmo que esse resultado possa ser encarado como um sucesso para os objetivos estabelecidos pela autarquia, o governo suíço entendeu que, de um ponto de vista objetivo, a resposta graduada é medida extrema, cujas consequências de longo prazo são impossíveis de ser avaliadas.

O relatório aponta ainda que a resposta graduada necessita da implementação de um amplo aparato estatal. Nesse sentido, os custos anuais de funcionamento da Hadopi são estimados em mais de 12 milhões de euros, de acordo com o orçamento público francês de 2011 do Ministério da Cultura e da Comunicação. O governo suíço questiona ainda a compatibilidade dos mecanismos de reposta graduada com as Convenções Internacionais, em especial o relatório conduzido pelo Conselho de Direitos Humanos das Nações Unidas que determinou que a interrupção do acesso à Internet é uma violação ao art. 19º, alínea 3 do Pacto Internacional dos Direitos Civis e Políticos.

9.3.2 Filtragem e bloqueio do acesso à Internet

O relatório do governo suíço aponta a importância da inserção do debate sobre medidas repressivas, principalmente quando se trata de provedores de acesso à Internet, na agenda de neutralidade da rede. Segundo os conselheiros, esse engajamento é fruto da necessidade de proteger a livre concorrência e os direitos fundamentais como liberdade de expressão, devido processo legal e privacidade. As filtragens e bloqueios operados por um provedor de acesso recebem as mesmas críticas e limitações da resposta graduada. Tais medidas são pouco compatíveis com direitos à liberdade de expressão e as tecnologias utilizadas para filtragem podem importar em sérios riscos à privacidade. Ainda, o fato de tais bloqueios não serem realizados por autoridades judiciais, mas sim por empresas privadas eleva de forma considerável a complexidade do problema e incentiva o debate sobre o papel do Poder Judiciário na resolução de casos que impliquem na reparação de danos ocorridos na Internet.

9.3.3 Licenças coletivas

A possibilidade de licenças coletivas de obras colocadas à disposição na Internet, sem fins comerciais e em conjunto com um sistema de remuneração, é apontada como uma abordagem permissiva possível. Essa solução traria a dupla vantagem de retirar os maiores usuários de *downloads* da ilegalidade, bem como de remunerar utilizações como o *streaming*. No entanto, segundo o relatório, grande parte da população suíça considera esse sistema de remuneração de certa forma "injusto". A compensação feita nesse modo só poderia ser considerada aceitável se levasse em consideração regras gerais de equidade. Ainda, faltaria compatibilizar esse regime com os acordos internacionais assinados pela Suíça. Convenções Internacionais, como as da OMPI, indicam que é direito exclusivo do autor disponibilizar suas obras *on-line*. As exceções e limitações a esse direito se fazem em casos excepcionais que não impliquem em obstáculo à exploração normal da obra. E, de qualquer forma, os titulares podem atingir esse resultado por meio de seus próprios contratos, não havendo necessidade de uma imposição legislativa para o mesmo.

O relatório do governo suíço questiona ainda a legitimidade das medidas repressivas de combate à violação de direitos autorais, afirmando que as mesmas devem obedecer a certos limites impostos por direitos fundamentais. Aponta também que muitos atores veem os direitos de autor como um entrave ao acesso à cultura e essa linha de entendimento chegou a ser, inclusive, apoiada em termos políticos pelo Partido Pirata Suíço, fazendo forte oposição à ideia de propriedade intelectual como forma de incentivar a produção cultural.

Apesar das críticas recebidas pelas licenças coletivas, o governo suíço aponta como desejável um acordo entre as grandes companhias de mídia, a sociedade de gestão coletiva e os provedores de acesso à Internet. No entanto, ao optar por uma regulamentação tecnicamente neutra, o legislador suíço já tirou o internauta da ilegalidade ao permitir a cópia para fins pessoais, independentemente da origem ilícita do arquivo copiado. Dessa forma, entende o relatório, não haveria necessidade de lei específica que regule o uso ilegal de obras na Internet.

ISBN 978-85-60062-60-7